RESUME TA

STRATEGI PERANCANGAN SISTEM KEAMANAN JARINGAN PADA LOCAL AREA NETWORK (LAN) DAN INTERNETWORKING BERBASIS FIREWALL

Suryo Adhi Wicaksono [1]
[1]Jurusan Teknik Infowmatika F.T. Universitas Komputer Indonesia

Jl. Dipati Ukur No. 112-114 Bandung 40132

ABSTRAK

Dalam dunia Internet yang telah berkembang sedemikian pesatnya, jumlah para pencuri data semakin meningkat. Setelah sebuah jaringan komputer berfungsi dan terhubung ke jaringan Internet, saat itulah *administrator* jaringan harus mulai bersiaga dan memikirkan strategi beserta cara-cara untuk meningkatkan keamanan jaringan komputer yang dimiliki. Dengan tingkat keamanan jaringan komputer yang tinggi, *user* pun akan merasa aman saat bekerja di jaringan komputer yang dimiliki. Strategi dalam keamanan jaringan komputer bertujuan untuk memaksimalkan sumber daya yang ada untuk mengamankan sistem jaringan komputer pada titik-titik yang tepat sehingga lebih efisien.

Hasil penelitian didapatkan bahwa perangkat lunak *sygate personal firewall* dapat menangkal trafik-trafik yang tidak inginkan. Kelemahan dari sygate personal firewall ini yaitu tidak dapat menangkal serangan virus komputer.

Kata kunci : Administrator, User, Sygate Personal Firewall

I. PENDAHULUAN

Jaringan komputer adalah sekumpulan komputer pribadi yang saling berhubungan antara satu dengan yang lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti *printer, hardisk*.[1] Selain itu jaringan komputer dapat diartikan sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri dari lebih dari satu komputer yang saling berhubungan. [(2,3)] Tujuan dibangunnya suatu jaringan komputer adalah membawa informasi secara tepat dan tanpa adanya kesalahan dari sisi pengirim (*transmitter*) menuju ke sisi penerima (*receiver*) melalui media komunikasi. Ada empat kategori utama jaringan computer, yaitu[4] : Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN) dan Global Area Network (GAN). Strategi dalam keamanan jaringan computer bertujuan untuk memaksimalkan sumber daya yang ada untuk mengamankan sistem jaringan computer pada titik-titik yang tepat sehingga lebih efisien. Ada beberapa strategi dasar dalam merancang sistem keamanan jaringan computer yaitu[5] : memberikan hak akses, membangun sistem keamanan secara berlapis, membuat satu jalur masuk, menggunakan enkripsi data dan *digital signature*, menggunakan *Stub Sub-network*, dan mencari titik lemah. Firewall digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan yang berfungsi membatasi control akses antara dua jaringan atau lebih khusus lagi antara jaringan internal dan jaringan global. Berdasarkan jenisnya, firewall dapat dibagi menjadi dua garis besar, yaitu *Packet Filtering* dan *Proxy*. Beberapa arsitektur firewall, yaitu : *Dual Homed Host, Bastion Host, Screened Host Gateway, Screened Subnet.*

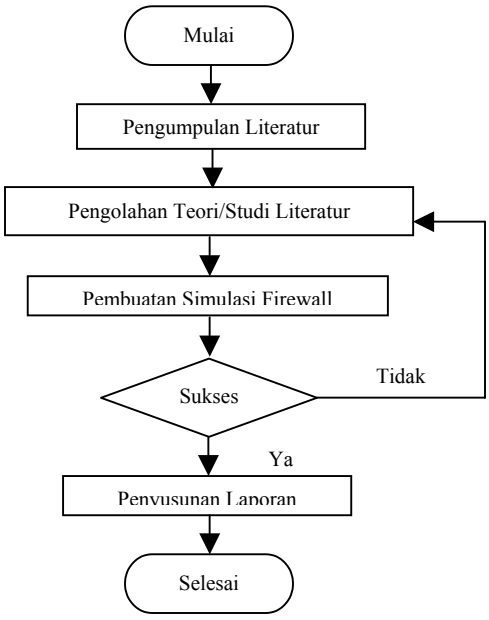
II. PROSEDUR EKSPERIMEN

Tujuan penelitian ini adalah untuk menerapkan strategi perancangan sistem keamanan jaringan computer LAN dan internetworking berbasis firewall.

Metode penelitian yang dilakukan adalah metode deskriptif dan studi literatur yaitu suatu metode yang meneliti status

sekelompok manusia, suatu objek, suatu kondisi atau suatu sistem pemikiran yang

bertujuan membuat deskripsi sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antar fenomena yang diselidiki. Sedangkan studi literature adalah penelitian dengan menggali data dari bahan-bahan tertulis (khususnya berupa teori-teori). Data dan fakta yang berupa pemikiran, teori, konsep atau penelitian yang dikemukakan oeleh berbagai sumber kemudian dibandingkan dan dianalisis satu sama lain, sehingga apa yang diuraikan pada tujuan penulisan skripsi dapat tercapai. Penelitian dilakukan di Universitas omputer Indonesia (UNIKOM) Bandung. Instrumen yang digunakan yaitu satu unit computer Pentium Celeron 850 Mhz dengan sistem operasi *Microsoft Windows XP*. Gambar 1 menggambarkan alur kerja penelitian

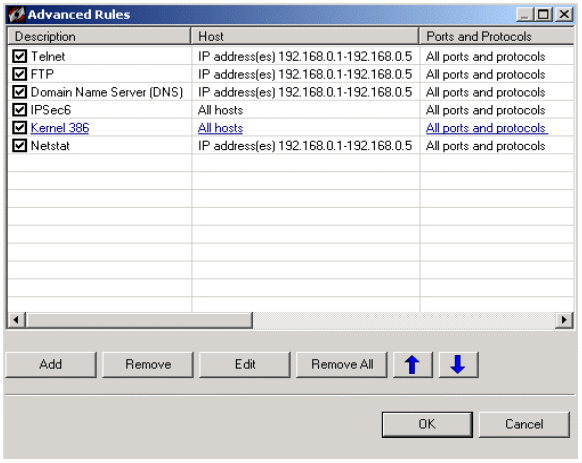


Gambar 1 Flowchart Penelitian

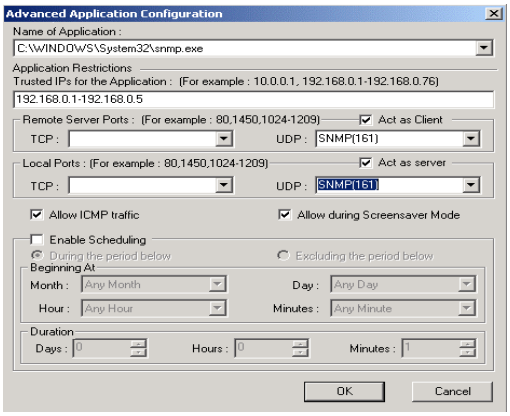
III. Hasil Analisa Strategi Perancangan Sistem Keamanan Jaringan pada Local Area Network (LAN) dan Internetworking berbasis Firewall

Ada beberapa strategi dasar dalam merancang sistem keamanan jaringan komputer yaitu : memberikan hak akses, membangun sistem keamanan secara berlapis, membuat satu jalur masuk akses data, menggunakan enkripsi data dan digital signature, menggunakan stub sub-network, mencari titik lemah.

Merencanakan sistem keamanan jaringan secara berlapis dapat menggunakan firewall sebagai salah satu alternatif. Merencanakan sistem keamanan jaringan dengan menggunakan firewall berkaitan erat dengan jenis fasilitas apa yang disediakan bagi para *user,* sejauh mana level resiko keamanan yang dapat diterima, serta berapa banyak waktu dan biaya yang diperlukan firewall umumnya terdiri dari bagian filter, filter ini berfungsi untuk membatasi akses, mempersempit port atau untuk memblok trafik tertentu. Firewall dapat diimplementasikan dalam bentuk perangkat keras atau dalam perangkat lunak. Pada skripsi ini penulis menggunakan perangkat lunak untuk digunakan sebagai firewall, perangkat lunak yang digunakan yaitu sygate personal firewall. Pada sygate personal firewall terdapat 3 level keamanan yaitu normal level ini akan meminta izin pada aplikasi baru selain yang terdapat pada daftar aplikasi yang telah dibuat untuk mengakses internet. Level block all yaitu level yang memblok semua trafik yang datang maupun yang keluar dari jaringan internal dan yang terakhir yaitu level allow all yaitu level yang mengizinkan semua trafik. Pada gambar 2 diperlihatkan aturan yang dibuat pada sygate personal firewall dan pada gambar 3 diperlihatkan konfigurasi IP yang dipercaya dan Port yang dipercaya.



Gambar 2 Aturan yang dibuat pada Sygate Personal Firewall



Gambar 3. Konfigurasi *Trusted IP* dan *Port*

Port umumnya digunakan pada *Transmission Contro Protocol* (TCP) tetapi dapat juga digunakan pada *User Datagram Protocol* (UDP). Port digunakan untuk mendefinisikan *transport address*. Pada tabel 1 dan tabel 2 terdapat *service, port* dan *status*. Service menyatakan pelayanan yang diizinkan atau yang diblok oleh sygate personal firewall, *Port* menyatakan pada port berapa service itu dilakukan sedangkan status menyatakan bahwa service dan port itu diizinkan atau diblok.

Tabel 1. Hasil Tes oleh Sygate Personal Firewall

Service	Ports	Status
FTP Data	20	Opened
FTP	21	Opened
SSH	22	Blocked
TELNET	23	Opened
SMTP	25	Blocked
DNS	53	Opened
DCC	59	Blocked
FINGER	79	Blocked
WEB	80	Opened
POP3	110	Opened
IDENT	113	Blocked
LOCATION SERVICE	135	Blocked
NetBIOS	139	Blocked
HTTPS	443	Opened
Server Message Block	445	Blocked
SOCKS PROXY	1080	Blocked
UPnP	5000	Blocked
WEB PROXY	8080	Blocked

Tabel 2. Hasil Tes untuk ICMP dilakukan oleh Sygate Personal Firewall.

Protocol	Type	Status
ICMP	8	Blocked

IV. Kesimpulan

Dari hasil penelitian yang dilakukan serta studi literatur terhadap strategi perancangan sistem keamanan jaringan, penulis mendapat kesimpulan bahwa :

1. Strategi perancangan keamanan jaringan komputer bertujuan untuk memaksimalkan sumber daya yang ada untuk mengamankan sistem jaringan komputer pada titik-titik yang tepat sehingga lebih efisien.
2. Ada beberapa strategi dasar dalam merancang sistem keamanan jaringan komputer yaitu memberikan hak akses, membangun sistem keamanan secara berlapis, membuat satu jalur masuk akses data, menggunakan enkripsi data dan digital signature, menggunakan stub sub-network dan mencari titik lemah
3. merencanakan keamanan jaringan komputer dengan firewall berkaitan dengan jenis fasilitas apa yang akan disediakan bagi para pemakai, sejauh mana level resiko keamanan yang bisa diterima, serta berapa banyak waktu dan biaya yang tersedia.
4. Hasil analisa sistem keamanan jaringan pada LAN dan Internetworking berbasis firewall dengan menggunakan perangkat lunak sygate personal

firewall (SPF) yaitu Pada SPF terdapat tiga level yaitu Normal, Block All dan Allow All. SPF dapat mengatur nomor IP, Port dan Protocol yang dapat digunakan oleh user.

REFERENSI

1. Wahana Komputer, Tim Penelitian Dan Pengembangan, Konsep Jaringan Komputer Dan Pengembangannya, Penerbit Salemba Infotek, 2003

2. B. Irawan, Diktat Kuliah Pengantar Jaringan Komputer, 2002

3. D. Heywood, Konsep dan Penerapan Microsoft TCP/IP, Penerbit ANDI Yogyakarta, 2001

4. S. Feit, TCP/IP: Architecture, Protocol, and Implementation, McGraw-Hill Inc, 1993

5. J.Yuliantoro dan O.W. Purbo, Strategi Merancang Sekuriti Jaringan Komputer Anda.

6. W.R Cheswick and S.M. Bellovin, Firewall and Internet Security: Repelling the Willy Hacker, Addison-Wesley Publishing Company, 1994

7. O.W. Purbo, TCP/IP: Standar, Desain dan Implementasi, Elexmedia Komputindo, 2002

8. O.W. Purbo dan T. Wiharjito, Keamanan Jaringan Internet, Elexmedia Komputindo, 2000

9. C. Brenton, Mastering Network Security, SybeX Inc,1999

10. C. Hare and K. Siyan, Internet Firewall and Network Security-2nd Edition, New Riders Publishing, 1996

11. S. McClure, J. Scambray and G. Kurtz, Hacking Exposed: Network Security Secret and Solution Third Edition, Osborne/McGraw-Hill, 2001