

# **INTERNET FIREWALL**

 Penerbit  
**GRAHA ILMU**

# **INTERNET FIREWALL**

**DONY ARIYUS**

## **INTERNET FIREWALL**

Oleh : Dony Ariyus

Edisi Pertama

Cetakan Pertama, 2006

Hak Cipta © 2006 pada penulis,  
Hak Cipta dilindungi undang-undang. Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apa pun, secara elektronis maupun mekanis, termasuk memfotokopi, merekam, atau dengan teknik perekaman lainnya, tanpa izin tertulis dari penerbit.



### **GRAHA ILMU**

Candi Gebang Permai Blok R/6

Yogyakarta 55511

Telp. : 0274-882262; 0274-4462135

Fax. : 0274-4462136

E-mail : [info@grahailmu.co.id](mailto:info@grahailmu.co.id)

Ariyus, Dony

INTERNET FIREWALL/Dony Ariyus

- Edisi Pertama - Yogyakarta; Graha Ilmu, 2006

x + 234 hlm, 1 Jil. : 23 cm.

ISBN-13: 978-979-756-144-4

ISBN-10: 979-756-144-5

1. Komputer

I. Judul



## KATA PENGANTAR

*P*embahasan tentang keamanan komputer sangatlah luas dan tidak habis-habisnya, dalam buku ini akan dibahas peran utama firewall dalam mengamankan sistem jaringan komputer, baik dari luar (internet) maupun dari dalam (intranet). Firewall yang berfungsi sebagai benteng utama dalam mengamankan data dan juga berfungsi sebagai packet filter untuk setiap packet yang masuk ke jaringan internal maupun sebaliknya.

Jika seseorang ingin menjebol suatu jaringan komputer, yang paling utama yang direncanakan adalah bagaimana supaya bisa untuk melewati firewall, begitu pentingnya firewall dalam element suatu jaringan komputer. Untuk menghindari hal ini, disain dan membangun suatu firewall harus dipikirkan kemungkinan yang ada.

Konfigurasi dan *security policy* (kebijakan keamanan) dari suatu firewall merupakan kunci utama untuk mendapatkan keamanan yang maksimum. Tujuan dari buku ini untuk memberikan informasi tentang seluk beluk dari firewall dan bagaimana membangun suatu firewall yang tangguh. Secara umum buku ini membahas hal-hal sebagai berikut:

- Melindungi Sistem Komputer, Packet dan Protocol, Packet Filtering, Firewall Technology, Internet Firewall ,Architecture Firewall, Maintaining Firewalls, System Proxy, Bastion Host, Security Policy, Serangan Pada Low-Level Protocol
- Dan masih banyak hal lainnya yang berhubungan dengan komputer security

Pembaca buku ini, sebaiknya telah mengenal dan mempelajari dasar-dasar mengenai TCP/IP, dan jaringan komputer secara umum, karena hal ini sangat membantu untuk mendapatkan pemahaman yang lebih mudah mengenai internet firewall.

Tidak ada gading yang tidak retak, tidak ada sesuatu yang sempurna, karena sekarang penulis juga sedang mendalami masalah keamanan. Terima kasih penulis ucapkan pada Drs. Jazi Eko Istiyanto, M.Sc., Ph.D dan Drs. Retanyo Wardoyo, M.S.c., Ph.D selaku Dosen yang memberikan mata kuliah keamanan komputer pada penulis di Program Pasca Sarjana ilmu komputer Universitas Gadjah Mada Yogyakarta.

Wassalam,  
Yogyakarta, 26 Juli 2006

Penulis  
Dony Ariyus





# DAFTAR ISI

<b>KATA PENGANTAR</b>	<b>v</b>
<b>DAFTAR ISI</b>	<b>vii</b>
<b>BAB 1 PENDAHULUAN</b>	<b>1</b>
1.1 Pengantar	1
1.1.1 Apa yang Akan diamankan	2
1.1.2 Data (informasi)	2
1.1.3 Sumber Daya	4
1.1.4 Reputasi	5
1.2 Melindungi Sistem Komputer	6
1.2.1 Jenis Serangan yang Sering Terjadi	6
1.2.2 Type-type Penyerang	11
1.3 Internet Firewall	14
1.3.1 Karakteristik Firewall	17
1.3.2 Fungsi dasar yang bisa dilakukan Firewall	18
1.3.3 Type Firewall	19
1.3.4 Network Address Translation (NAT)	30
1.3.5 Strategi Keamanan Internet	33
<b>BAB 2 PACKET DAN PROTOKOL</b>	<b>37</b>
2.1 Packet	37
2.1.1 KarakteristikProtokol	38
2.1.2 Packet TCP/IP	44

2.2	IP (Internet Protokol)	47
2.2.1	IP Multicast and Broadcast	47
2.2.2	Internet Protokol (IP) Option	49
2.2.3	IP Fragmentation	49
2.3	Protocols Above IP	54
2.3.1	Tansmission Control Protokol (TCP)	54
2.3.2	User Datagram Protokol (UDP)	58
2.3.3	Internet Control Message Protokol (ICMP)	60
2.3.4	IP over IP	69
2.4	Protokol below IP	70
2.5	Application Layer Protocol	71
2.6	IP versi 6 (IPv6)	71
2.6.1	Layanan Keamanan IPv6	81
2.7	Non-IP Protocols	86
2.8	Serangan pada Low-level Protokol	86
2.8.1	Port Scanning	86
2.8.2	Mencari Kelemahan	90
2.8.3	IP Spoofing	91
2.8.4	Serangan yang Bisa Terjadi Pada Protocol ICMP	98
<b>BAB 3</b>	<b>FIREWALL TEKNOLOGI</b>	<b>115</b>
3.1	Pendahuluan	115
3.2	Packet Filtering	117
3.2.1	Apa yang bisa dilakukan oleh packet filter?	118
3.2.2	Dasar Packet Filtering	120
3.2.3	Packet Filter Dinamis	121
3.2.4	Protocol Checking	122
3.3	Packet Filter Tip dan Trick	123
3.3.1	Edit Filtering Rules Offline	123
3.3.2	Reload Rule Pada Setiap Koneksi	124
3.3.3	Replace Packet Filters Secara Otomatis	124



3.3.4	Selalu Menggunakan IP Address, Tidak Hostname	125
3.3.5	Memberikan password pada packet filter	125
3.4	Filter dengan Menggunakan Address	125
3.5	Filter dengan Menggunakan Service	126
3.5.1	Outbound Telnet Service	126
3.5.2	Inbound Telnet Service	127
3.6	Arsitektur Firewall	129
3.6.1	Single-Box	129
3.6.2	Screening Router	130
3.6.3	Dual-Homed Host	131
3.6.4	Multiple-Purpose Boxes	132
3.6.5	Screened Host	133
3.6.6	Screened Subnet	134
3.6.7	Multiple Screened Subnets	136
3.7	Sistem Proxy	139
3.7.1	Bagaimana Proxy Berkerja	149
3.7.2	Proxy Server Layer Network	150
3.7.3	Proxy Server Pada Level Sirkuit	151
3.7.4	Konvesi Client Untuk Menggunakan SOCKS	156
<b>BAB 4</b>	<b>BASTION HOSTS</b>	<b>159</b>
4.1	Pendahuluan	159
4.2	Macam-macam bastion host	162
4.3	Memilih Mesin	164
4.3.1	Sistem Operasi	164
4.3.2	Megapa Mesin Bastion Host Tidak Optimal	166
4.3.3	Konfigurasi Hardware	166
4.4	Memilih Layanan Service Bastion Host	167
4.4.1	Multiple Services atau Multiple Hosts	168
4.5	Membangun Suatu Bastion Host	170
4.6	Menjalankan Bastion Host	171
4.6.1	Apakah Sistem Berjalan Dengan Normal	172

4.6.2	Software yang digunakan untuk Membantu Aktifitas Monitoring	172
4.7	Unix dan Linux Bastion Host	173
4.7.1	Unix yang Aman	174
4.7.2	Setting Up System Logs pada UNIX	174
4.8	Windows NT dan Windows 2000 Bastion Hosts	175
4.8.1	Windows NT yang Aman	176
4.8.2	Setting Up System Logs pada Windows NT	177
<b>BAB 5</b>	<b>MENJAGA SISTEM TETAP AMAN</b>	<b>179</b>
5.1	Securiy Policy (Kebijakan Keamanan)	179
5.2	Maintaining Firewalls	186
5.2.1	Housekeeping	187
5.2.2	Memonitor Sistem	188
5.2.3	Up to Date Sistem	194
	<b>DAFTAR PUSTAKA</b>	<b>197</b>
	<b>LAMPIRAN</b>	<b>199</b>
	Lampiran 1 : Service yang Umum dari TCP dan UDP	201
	Lampiran 2 : Sumber-sumber Informasi Keamanan	213
	Lampiran 3 : Top-Level Domains	227
	TENTANG PENULIS	233

-oo0oo-





## TENTANG PENULIS

**D**ONY ARIYUS, dilahirkan 26 tahun yang lalu di Sungai-Penuh, penulis sudah memiliki minat terhadap ilmu komputer sejak bangku sekolah menengah, dan melanjutkan pendidikan S1 di jurusan Sastra Inggris konsentrasi study pada bidang linguistic, waktu S1 penulis mengikuti pelatihan, kursus, dan banyak belajar dari buku-buku text komputer secara autodidact, karena minat akan Ilmu Komputer begitu besar akhirnya penulis memutuskan untuk mengambil Study S2 pada Program Pasca Sarjana Ilmu Komputer di Universitas Gadjah Mada Yogyakarta.

Dengan modal bahasa inggris, motivasi yang kuat, serta sifat yang suka otak-atik komputer membuat penulis bisa lebih cepat mempelajari, memahami, dan mempraktekkan Ilmu Komputer, khususnya pada bidang computer security dan security networking yang di dapat secara formal di jenjang pendidikan S2. sekarang penulis sedang menyelesaikan thesis dengan judul penelitian “ **ANALYSIS, USING INTRUSION DETECTION SYSTEM AT COMPUTER NETWORKING**”

-oo0oo-