OPTIMALISASI JARINGAN MENGGUNAKAN FIREWALL

Fajar Adhi Purwaningrum[1], Agus Purwanto[2], Eko Agus Darmadi[3]

[1,2,3] Politeknik Tri Mitra Karya Mandiri
Blok Semper Jomin Baru, Kotabaru, Cikampek - Karawang
ekoagus.darmadi@gmail.com
f.apurwaningrum@yahoo.co.id[1], aguspurwanto44@yahoo.com[2],
ekoagus.darmadi@gmail.com[3]

ABSTRAK

Firewall membatasi siapa saja yang berhak mengakses suatu internet dalam jaringan, dan siapa saja yang harus diizinkan dan tidak diizinkan untuk lewat, hal ini biasa disebut dengan filtering. Firewall pada jaringan, dapat mematau aktifitas suatu jaringan**.** Dari pengujian yang dilakukan, firewall terbukti dapat melindungi suatu jaringan dengan melakukan filtering dan proxy. Bertujuan untuk optimalisasi sistem firewall security menggunakan dual home host, screened host, dan screened subnet pada wide area network. Firewall merupakan suatu perangkat keamanan jaringan yang memperkenankan berbagai bagian ruas jaringan untuk melaksanakan komunikasi antara satu dengan yang lainnya sesuai dengan definisi kebijakan keamanan yang telah diterapkan sebelumnya. Firewall peka terhadap kesalahan konfigurasi dan kegagalan untuk menerapkan kebijakan, sehingga diperlukan tambahan atau peningkatan keamanan lain.

Kata Kunci: ***Firewall, Keamanan Sistem Komputer, Internet***

ABSTRACT

Firewalls limit anyone who has the right to access an internet in a network, and anyone who must be allowed and not allowed to pass, this is usually called filtering. A firewall on the network, can monitor the activity of a network. From the tests carried out, the firewall is proven to protect a network by filtering and proxies. Aiming to optimize the firewall security system using dual home hosts, screened hosts, and screened subnets on wide area networks. Firewall is a network security device that allows various parts of a network segment to carry out communication between one another in accordance with the definition of a security policy that has been applied previously. Firewalls are sensitive to configuration errors and failure to implement policies, so that additional security or enhancements are needed.

Keywords: Firewall, Computer System Security, Internet

1. PENDAHULUAN

Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya Firewall merupakan solusi untuk mengatasi keamanan di dalam dunia internet baik itu keamanan komputer maupun keamanan jaringan yang banyak dipenuhi dengan berbagai ancaman baik dari dalam maupun dari luar. Dengan suatu konfigurasi yang tepat pada firewall maka kemungkinan untuk mengamankan suatu data atau komputer pada jaringan menjadi jauh lebih aman (Van Busten, 2009).

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap negara maju maupun negara berkembang terdapat jaringan komputer untuk memperlancar arus informasi di dalam pemerintahan negara 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 (MikroTik, 2010).

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 port-port 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 (Haryanto dan Riadi, 2014).

Konfigrasi suatu firewall yang pertama adalah penentuan policy atau kebijakan firewall tersebut tentang apa saja yang akan dikenai kebijakan tersebut, siapa saja yang akan dikenai kebijakan tersebut dan layanan-layanan yang dibutuhkan tiap individu tersebut. Kemudian menentukan port-port yang digunakan oleh berbagai protokol dan membuka port-port tersebut kedalam firewall, dan juga membuka port yang digunakan untuk file sharing dan request ping. Selanjutnya adalah menentukan suatu konfigurasi yang tepat dan sesuai dengan keadaan jaringannya. Screened subnet merupakan konfigurasi yang paling tinggi tingkat keamanannya(Van Busten, 2009).

Dengan konfigurasi tersebut memungkinkan firewall kita dapat menigkatkan keamanan yang jauh lebih baik dari ancaman-ancaman internet. Namun tidak menutup kemungkinan bahwa jaringan kita tetap dapat diserang oleh hacker yang serangannya sangat terarah. Namun lebih baik sedikit terlindungi daripada tidak sama sekali.

2. LANDASAN TEORI

2.1 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang di desain untuk dapat berbagi sumber daya, berkomunikasi, dan dapat mengakses informasi.dengan informasi dan data melalui kabel sehingga memungkinkan pengguna dapat saling bertukan informasi maupun data (Romadhona, 2012).

2.1.1. Jenis-Jenis Jaringan

Ada 3 macam jenis jaringan, yaitu :

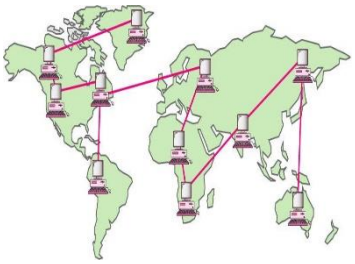
1. Lokal Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)

2.1.2. WAN (*Wide Area Network*)

Wide Area Network merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara (MikroTik, 2010).

Adapun beberapa karakteristik dari jaringan WAN, diantaranya sebagai berikut ini :

1. WAN digunkan untuk menghubungkan jaringan yang sangat luas.
2. Jaringan WAN akan melibatkan Operator telekomunikasi
3. Menggunakan koneksi serial



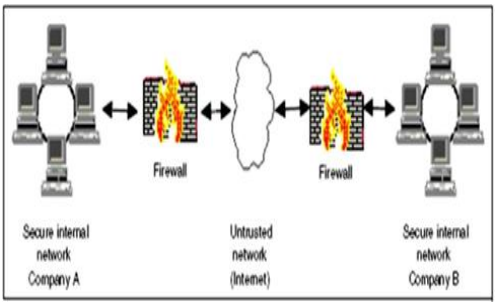
Gambar 1 Jaringan WAN

2.2 Firewall

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 (Angela).

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. Diantara kegunaannya yaitu :

1. Membatasi gerak orang yang masuk ke dalam jaringan internal
2. Membatasi gerak orang yang keluar dari jaringan internal
3. Mencegah penyerang mendekati pertahanan yang berlapis



Gambar 2 Firewall

2.2.1. Tugas Tugas Firewall

Firewall secara umum di peruntukkan untuk melayani :

1. Mesin/Komputer
2. Jaringan
3. Terpenting: harus dapat mengimplementasikan kebijakan security di jaringan (site security policy)
4. Melakukan filtering
5. Merekam atau mencatat serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan security (Van Busten, 2009).

Beberapa hal yang tidak dapat dilakukan oleh firewall :

1. Firewall tidak bisa melindungi dari serangan orang dalam
2. Firewall tidak bisa melindungi serangan yang tidak melalui firewall tersebut (tidak melalui chocke point).
3. Firewall tidak bisa melindungi jaringan internal terhadap serangan-serangan model baru.

Tugas tugas firewall yaitu di antaranya yang pertama adalah memfilter jaringan yang tidak di inginkan dengan kebijakan sistem security di jaringan (site security policy). yang kedua adalah semua trafik yang ada untuk dilewatkan firewall bagi semua pemberian dan pemanfaatan layanan informasi (Van Busten, 2009).

2.2.2. Teknik Yang Digunakan Firewall

1. Service Control (kendali terhadap layanan)
2. Direction Conrol (kendali terhadap arah)
3. User control (kendali terhadap pengguna)
4. Behavior Control (kendali terhadap perlakuan)

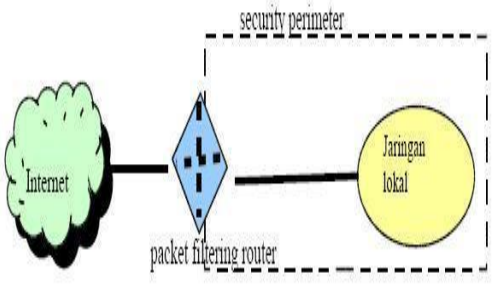
2.2.3. Tipe-Tipe Firewall

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 (MikroTik, 2010).

   Adapun kelemahannya adalah cukup rumitnya untuk mensetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi. Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

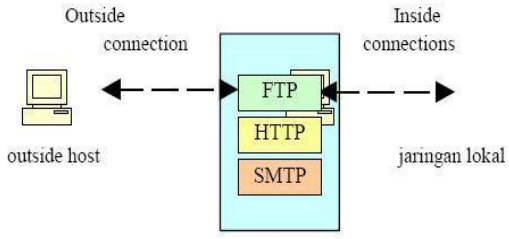
   1) IP address spoofing
   2) Source routing attacks
   3) Tiny Fragment attacks



Gambar 3 Packet Filtering

2. Application-Level Gateway

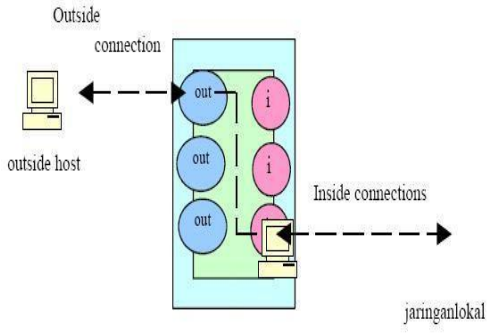
Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi.



Gambar 4 Application Gateway

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) (Van Busten, 2009).



Gambar 5 Circuit Gateway

3. HASIL DAN PEMBAHASAN

3.1 Merencanakan Jaringan Dengan Firewall

Merencanakan sistem firewall pada jaringan, berkaitan erat dengan jenis fasilitas apa yang akan disediakan bagi para pemakai, sejauh mana level resiko-security yang bisa diterima, serta berapa banyak waktu, biaya dan keahlian yang tersedia (faktor teknis dan ekonomis). Firewall umumnya terdiri dari bagian filter (disebut juga screen atau choke) dan bagian gateway (gate). Filter berfungsi untuk membatasi akses, mempersempit kanal, atau untuk memblok kelas trafik tertentu.

Terjadinya pembatasan akses, berarti akan mengurangi fungsi jaringan. Untuk tetap menjaga fungsi komunikasi jaringan dalam lingkungan yang ber-firewall, umumnya ditempuh dua cara :

Pertama, bila kita bayangkan jaringan kita berada dalam perlindungan sebuah benteng, komunikasi dapat terjadi melalui pintu-pintu keluar benteng tersebut. Cara ini dikenal sebagai packet-filtering, dimana filter hanya digunakan untuk menolak trafik pada kanal yang tidak digunakan atau kanal dengan resiko-security cukup besar, sedangkan trafik pada kanal yang lain masih tetap diperbolehkan.

Berbagai kebijakan dapat diterapkan dalam melakukan operasi packet filtering. Pada intinya, berupa mekanisme pengontrollan data yang diperbolehkan mengalir dari dan/atau ke jaringan internal, dengan menggunakan beberapa parameter yang tercantum dalam header paket data: arah (inbound atau outbound), address asal dan tujuan, port asal dan tujuan, serta jenis protocol transport.

Cara kedua, menggunakan sistem proxy, dimana setiap komunikasi yang terjadi antar kedua jaringan harus dilakukan melalui suatu operator, dalam hal ini proxy server. Beberapa protokol, seperti telnet dan SMTP (Simple Mail Transport Protocol), akan lebih efektif ditangani dengan evaluasi paket (packet filtering).

Dalam jaringan yang menerapkan sistem proxy, hubungan komunikasi ke internet dilakukan melalui sistem pendelegasian. Komputer-komputer yang dapat dikenali oleh internet bertindak sebagai 'wakil' bagi mesin lain yang ingin berhubungan ke luar. Proxy server untuk (kumpulan) protokol tertentu dijalankan pada dual-homed host atau bastion-host.

Gambar 6 Sistem Proxy

3.2 Optimalisasi Jaringan dengan Firewall

Untuk melakukan optimalisasi suatu firewall ada beberapa hal yang perlu diperhatikan. Diantaranya :

Yang pertama kita perlu menentukan Policy atau kebijakan firewall terebut. Kerena penentuan policy atau kebijakan merupak hal yang sangat penting, baik atau buruknya sebuah firewall sangat ditentukan oleh policy atau kebijakan yang diterapkan. Penentuan kebijakan tersebut meliputi :

1. Menentukan apa saja yang perlu dilayani. Artinya apa saja yang akan dikenai kebijakan yang akan kita buat.
2. Menentukan individu atau kelompok-kelompok yang akan dikenai policy atau kebijakan tersebut.
3. Menentukan layanan-layanan yang dibuthkan oleh tiap-tiap individu atau kelompok yang menggunakan jaringan.
4. Berdasarkan setiap layanan yang digunakan oleh individu atau kelompok tersebut akan ditentukan bagaimanan konfigurasi terbaik yang akan membuatnya semakin nyaman.
5. Menerapkan semua policy atau kebijakan tersebut.

Berikutnya dapat menganalisis daftar port-port yang digunakan oleh berbagai protocol dan membuka port-port tersebut kedalam firewall dan port-port terebut harus tepat. Server web biasanya diidentifikasikan melalui port 80, FTP (File Transfer Protocol) melalui port 21, SSH melaui port 22. Port ini menunjukan port mana yang harus dibuka di sisi server web. Pada PC port-port yang perlu dibuka adalah untuk membuat koneksi keluar, settingan untuk itu biasanya telah dilakukan oleh firewall secara otomatis ketika ketika kita menjalankan sebuah program yang memerlukan koneksi ke internet

Pada dasarnya, semakin banyak port yang terbuka pada firewall maka semakin tidak aman PC tersebut, terutama pada file dan printer-sharing di bawah Windows sering menemukan dan memanfaatkan titik-titik kelemahan yang ada. Jika kita sedang menggunakan notebook yang terhubung ke hotspot umum tutup port-port yang terbuka. Firewall modern akan secara otomatis mengenali jaringan dan mengkonfigurasi diri sendiri seseuai dengan situasi. Kebanyakan firewall masa kini menawarkan fungsi setting otomatis untuk file dan printer-sharing.

Apabila kita terkoneksi ke internet melalui sebuah router ada baiknya jika mengkonfigurasi router tersebut. Settingan router yang perlu dirubah adalah fungsi Port Forwarding yang harus diaktifkan, karena pada kebanyakan router suatu fungsi Port Forwarding biasanya telah dimatikan secara default. Dengan konfigurasi yang tepat, router akan menolak paket IP dengan pengirim palsu.

Pengoptimalisasian firewall yang berikutnya adalah menentukan konfigurasi suatu firewall dengan tepat. Ada beberapa konfigurasi firewall :

[1] Dual-homed host

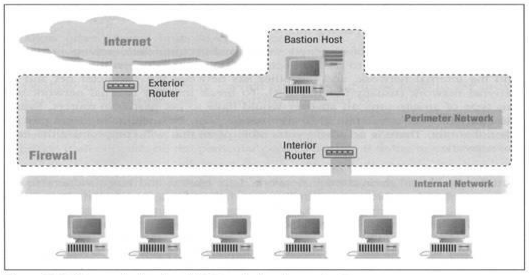


Figure 4–5: Screened subnet architecture (using two routers)

Gambar 7 Dual-homed host

Dual homed host bisa menjadi router, namun untuk menjadi firewall lalu lalu-lintas IP dalam arsitektur ini benar-benar di-blok. Jadi kalau ada paket yang mau keluar masuk, harus lewat proxy.

[2] Screened Host

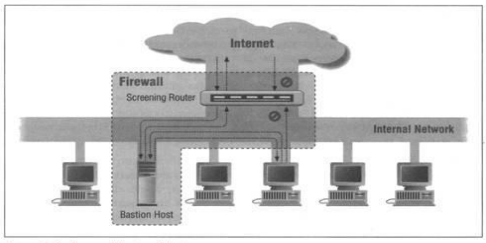


Figure 4–4: Screened host architecture

Gambar 8 Screened Host

Menggunakan bastion host yang diletakkan dalam intranet, dan seluruh komunikasi keluar masuk harus melalui proxy pada bastion dan kemudian melalui screening router. Bastion host merupakan sistem/bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator.atau dapat di sebut bagian terdepan yang dianggap paling kuat dalam menahan serangan.

Sekilas terlihat bahwa dual-homed architecture lebih aman, tetapi dalam prakteknya banyak kegagalan sistem yang memungkinkan paket lewat dari satu sisi ke sisi lainnya dalam dual homed architecture. Jadi alasan utama menggunakan screened host architecture adalah karena router lebih mudah diamankan ketimbang sebuahv komputer/host. Kejelekan utama kedua-duanya adalah mereka memiliki ‘single point of failure’.

[3] Screened Subnet

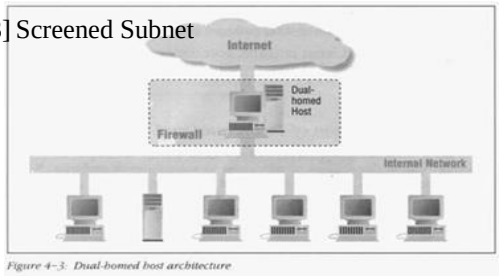


Figure 4–3: Dual-homed host architecture

Gambar 9 Screened Subnet

Alasan mengapa Bastion host sering menjadi target serangan. Karena idenya adalah kalau bastion host berhasil dibobol, jangan sampai penyerang masuk ke dalam jaringan internal. Oleh karena itu bastion host diletakkan di perimeter network. Untuk membobol jaringan, hacker harus menyerang exterior router dan interior router. Ada juga yang memiliki perimeter berlapis, dimana syaratnya agar efektif adalah sistem pertahan tiap lapis harus berbeda-beda.

Perimeter network yaitu kalau ada orang yang berhasil menembus ke exterior router dan bastion, maka sang penyerang hanya bisa melihat paket yang berkeliaran di perimeter network saja. Jadi lalu-lintas komunikasi pada jaringan internal (yang relatif sensitif) tidak dapat dilihat oleh penyerang dari perimeter network.

Bastion host Bertindak sebagai titik masuk koneksi dari luar, termasuk SMTP, FTP dan DNS. Sedangkan untuk melakukan koneksi dari client ke server di Internet dapat dilakukan dengan 2 cara:

1. Mengizinkan router-router agar klien bisa berhubungan dengan server Internet secara langsung.
2. Menggunakan proxy server pada bastion.

Interior router melindungi internal network dari Internet dan perimeter network. Sebaiknya lalu-lintas yang diizinkan antara bastion dengan client, hanyalah yang

penting-penting saja. Misalnya hubungan SMTP antara bastion dengan mail server internal. Perhatikan komputer server internal apa saja yang terhubung dengan bastion, karena itulah yang akan menjadi target serangan jika bastion berhasil dihancurkan oleh hacker.

Exterior router pada prakteknya mengizinkan banyak paket keluar, dan hanya sedikit memfilter paket masuk. Namun, biasanya untuk screening network internal, settingnya sama antara internal dan external router. Tugas utama external router adalah untuk memblok paket yang memiliki alamat yang palsu dari luar (karena berusaha menyamar dengan alamat IP salah satu host dalam internal network). Karena pasti dari Internet. Kenapa tidak di internal router? Karena masih bisa dari perimeter net yang sedikit lebih trusted.

4. KESIMPULAN

1) Penentuan policy merupakan komfigurasi utama dalam suatu firewall, kemudian menentukan port port yang di gunakan oleh berbagai protokol dan membuka port tersebut dengan firewal, dan juga membuka membuka port yang di gunakan untuk file sharing dan request ping. Kemudian menentukan suatu konfigurasi ini di gunakkan dua buah paket filtering router.
2) Dengan konfigurasi tersebut memungkinkan firewall dapat meningkatkan keamanan yang jauh lebih baik dari ancaman-ancaman internet. Namun tidak menutup kemungkinan bahwa jaringan kita tetap dapat diserang oleh hacker yang serangannya sangat terarah. Namun kita lebih baik mengurangi serangan tersebut daripada tidak sama sekali.
3) Firewall dapat mengoptimalisasikan jaringan sehingga dapat membentenggi ancaman-ancaman yang terjadi di dunia internet dan membuat nyaman bagi pengguna internet.
4) Mengoptimalisasikan firewall pada jaringan dapat mengurangi ancaman-ancaman yang ada di dalam dunia internet dan kita menjadi merasa lebih nyaman menjelajahi dunia internet.

DAFTAR PUSTAKA

D. Angela, “Optimasi Jaringan Wireless Lan (Studi Kasus Di Kampus Ithb Bandung),” no. 80.

Frendi Yusroni Romadhona, “Optimalisasi Jaringan Wireless Dengan QoS Berbasis Algoritma Hierarchical Token Bucket (HTB),” 2012.

M. Van Busten, “Optimalisasi Firewall Pada Jaringan Skala Luas,” *Jar. Komput.*, pp. 1–23, 2009.

MikroTik, “Optimalisasi manajemen Jaringan Dengan Menggunakan Mikrotik routerOS,” *Access*, p. 491, 2010.

M. Dedy Haryanto and I. Riadi, “ANALISIS DAN OPTIMALISASI JARINGAN MENGGUNAKAN TEKNIK LOAD BALANCING (Studi Kasus : Jaringan UAD Kampus 3),” *Jar. Komput.*, vol. 2, no. 2, pp. 1370–1378, 2014.