ISSN 1907-9044 (Print)
ISSN 2614-882X (Online)

OPTIMALISASI FIREWALL PADA SISTEM JARINGAN KOMPUTER KANTOR

Arief Tri Arsanto

Program Studi Tekik Informatika, Universitas Yudharta Pasuruan
e-mail: ariftriarsanto@gmail.com

ABSTRAK

Hampir setiap perusahaan atau kantor memiliki Jaringan komputer yang memfasilitasi aliran informasi di dalamnya. Internet berinteraksi dengan komputer melalui perkembangan teknologi. Namun, ada banyak serangan yang dapat merusak komputer, seperti virus, trojan horse, dan hacker. Keamanan komputer dan jaringan memainkan peran penting dalam kasus tersebut. Konfigurasi firewall yang tepat dapat mengurangi ancaman ini. Ada tiga jenis konfigurasi firewall: sistem firewall host yang disaring (single home fortress), sistem firewall host yang difilter (dual home fortress), dan firewall subnet yang difilter. Selain mengkonfigurasi firewall yang sesuai untuk menghubungkan ke Internet, mengkonfigurasi port firewall memungkinkan Anda untuk memfilter paket data yang masuk sesuai dengan pedoman. Arsitektur firewall ini digunakan untuk optimasi firewall di jaringan Anda.
Kata kunci: *Firewall*, Jaringan Computer

Pendahuluan

Selain berkontribusi terhadap kehidupan, internet juga menjadi ancaman. Ancaman bahkan lebih menakutkan dari dunia maya, mulai dari serangan virus, trojan horse, phishing hingga cracker yang dapat meretas sistem keamanan komputer. Menghubungkan ke Internet seperti membuka pintu komputer untuk diakses semua orang. Dari pintu di mana peretas dapat masuk dan dengan mudah membingungkan dan bahkan mengontrol sistem komputer. Anda harus dapat membuat keputusan yang kredibel dan tidak dapat diandalkan. Itu berasal dari sumber tepercaya dan dapat dijalankan dengan aman.

Pada dasarnya, komputer Anda membutuhkan benteng yang dapat melindungi komputer Anda dari ancaman Internet yang berbahaya. Keamanan komputer dan jaringan, yang terhubung ke Internet, perlu direncanakan dengan baik untuk melindungi sumber daya dan investasi. Informasi (data) dan layanan telah menjadi produk yang sangat penting. Kemampuan mengakses dan menyampaikan informasi dengan cepat dan akurat sangat penting bagi organisasi, perusahaan, atau individu

Jaringan Komputer

Instalasi komputer terdiri atas, printer, dan perangkat lain yang terhubung. Data Informasi dikirim melalui kabel sehingga pengguna komputer dapat bertukar data, mencetak pada printer yang sama, dan menggunakan perangkat keras / perangkat lunak jaringan pada saat yang sama. Setiap komputer, printer, atau periferal yang terhubung ke jaringan Anda disebut node. Jaringan komputer memiliki dua, sepuluh, ribuan, dan bahkan jutaan node. Sebuah jaringan terdiri dari dua atau lebih komputer yang saling berinteraksi dan dapat berbagi sumber daya seperti CDROM, printer, dan file, dan saling berkomunikasi secara elektronik.

Firewall

Internet adalah komputer paling terbuka di dunia, dan tidak ada tanggung jawab bila terjadi kebocoran keamanan jaringan. Artinya, jika operator tidak memantau administrasi sistem, kemungkinan besar akan mudah diakses oleh siapa saja yang belum diundang ke jaringan yang terhubung ke Internet. Merupakan tanggung jawab masing-masing operator jaringan untuk

meminimalkan risiko ini. Pilihan dan strategi diferensiasi untuk administrator jaringan ini dapat sangat membantu dalam menentukan apakah jaringan Anda rentan terhadap penyusupan. Firewall adalah alat untuk mengimplementasikan suatu kebijakan keamanan (security policy). Kebijakan keamanan didasarkan pada keseimbangan antara fasilitas yang disediakan dan keamanannya.

Semakin ketat pedoman keamanan, semakin kompleks konfigurasi layanan informasi dan semakin sedikit fitur yang tersedia di jaringan. Di sisi lain, semakin mudah bagi orang luar untuk membobol sistem, semakin banyak opsi atau konfigurasi yang tersedia (akibat langsung dari pedoman keamanan yang lemah). Di dunia nyata, firewall adalah dinding yang memisahkan ruangan dan mencegah api di satu ruangan menyebar ke ruangan lain.

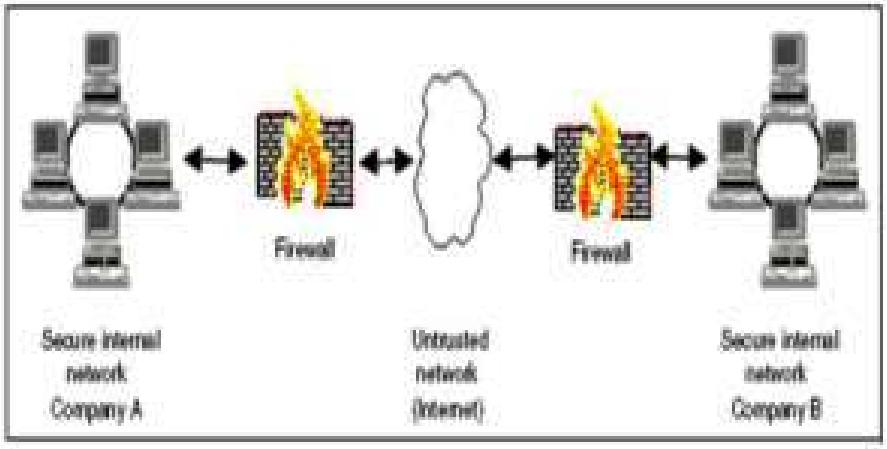


Figure 266. A firewall illustration

Sumber : Artikel Internet (Firewall)

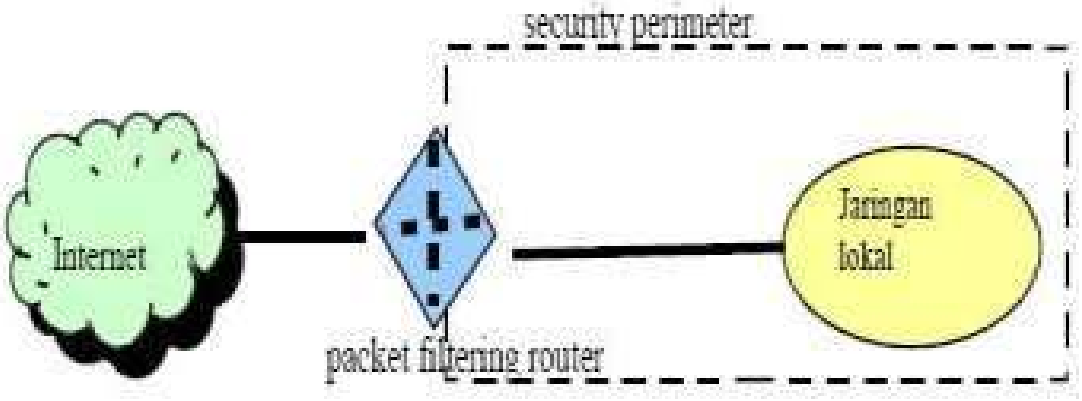
Tipe – Tipe Firewall

1. Packet Filtering Router

Pemfilteran paket diimplementasikan dengan mengelola semua paket IP, terlepas dari apakah paket tersebut tiba, melewati, atau dialamatkan oleh paket tersebut. Jenis paket ini memutuskan apakah akan menerima, menikmati atau menolak. Pemfilteran paket dikonfigurasi untuk memfilter paket yang dikirim dalam dua arah (ke dan dari jaringan lokal). Aturan yang digunakan didasarkan pada IP dan transport header, seperti alamat awal (IP) dan tujuan (IP), protokol transport (UDP, TCP), dan nomor port yang digunakan. Keuntungan dari jenis ini adalah mudah diimplementasikan, transparan bagi pengguna, dan relatif cepat. Kekurangannya adalah cukup rumit untuk mengatur paket yang akan difilter dengan benar, dan lemah dalam hal otentikasi. Serangan yang dapat terjadi pada firewall jenis ini adalah:

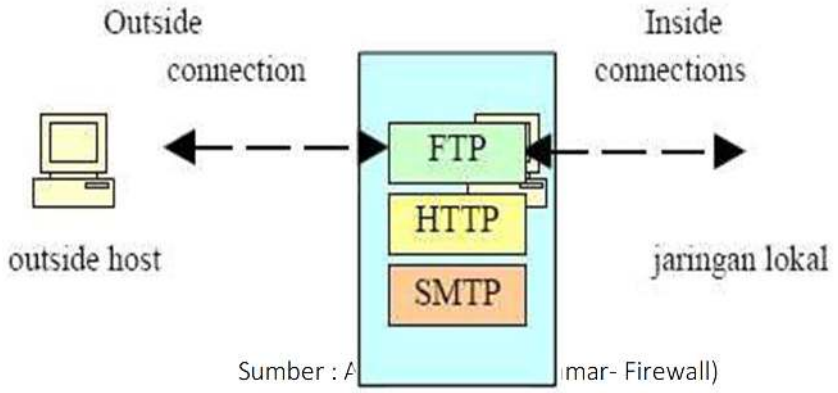
a. IP Address Spoofing: Penyusup (penyusup eksternal dapat melakukan ini dengan memasukkan alamat IP dari jaringan lokal yang dijangkau untuk melewati firewall.
b. Serangan Perutean Sumber: Jenis serangan ini tidak menganalisis informasi perutean IP sumber dan dapat melewati firewall.
c. Serangan Fragmen Kecil: Penyusup memecah IP menjadi fragmen yang lebih kecil dan memaksa mereka untuk bertukar informasi menggunakan header TCP.

Serangan ini dirancang untuk menipu layanan jahat yang mengandalkan informasi dari header TCP. Mengharapkan hanya fragmen pertama yang diperiksa dan sisanya lolos tanpa hambatan. Ini dapat diselesaikan dengan menolak semua paket dengan protokol TCP dan fragmen IP (bagian IP) offset = 1.



2. Application-Level Gateway

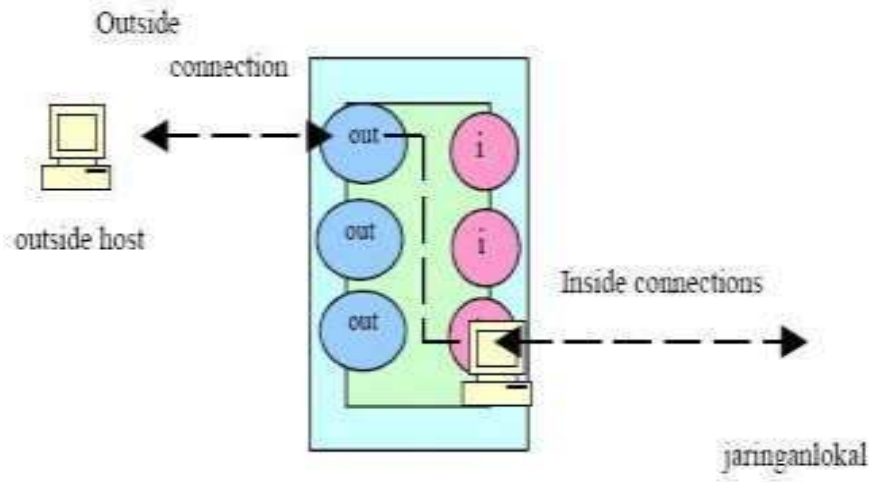
Gateway tingkat aplikasi, digunakan untuk memperkuat / mengalirkan aplikasi saat ini. Tipe ini mengatur semua koneksi yang menggunakan lapisan aplikasi seperti FTP, HTTP, dan GOPHER. Jika pengguna menggunakan aplikasi seperti FTP untuk akses jarak jauh, gateway meminta alamat host jarak jauh kepada pengguna. Ini akandiakses. Ketika pengguna memberikan ID pengguna dan informasi lain yang sesuai, gateway terhubung ke aplikasi. Tinggal di host jarak jauh dan mentransfer data. Jika data tidak cocok firewall tidak menyimpan data. Selanjutnya, kofigurasi jenis firewall ini hanya pada beberapa aplikasi melewati firewall. Keuntungannya adalah relatif lebih aman daripada router tipe packet filtering, lebih mudah untuk memeriksa dan merekam semua aliran data yang masuk di level aplikasi. Yang akan menghasilkan dua koneksi antara pengguna dan gateway, di mana gateway akan memeriksa dan memantau semua arus dari kedua arah.



3. Circuit-level Gateway

Tipe ini berupa sistem yang berdiri sendiri atau fitur khusus yang terbentuk dari gateway pada level aplikasi. Jenis ini tidak mengizinkan koneksi TCP ujung ke ujung (langsung). Cara kerjanya: Gateway mengelola dua koneksi TCP. Satu dengan TCP pada pengguna lokal (host internal) dan yang lainnya dengan pengguna TCP eksternal (host eksternal). Ketika dua koneksi dibuat, gateway mengalirkan segmen TCP dari satu koneksi ke koneksi lain tanpa memeriksa

isinya. Fitur itu adalah tempat hubungan diizinkan. Penggunaan jenis ini biasanya karena ketidakpercayaan administrator terhadap pengguna internal (internal user).



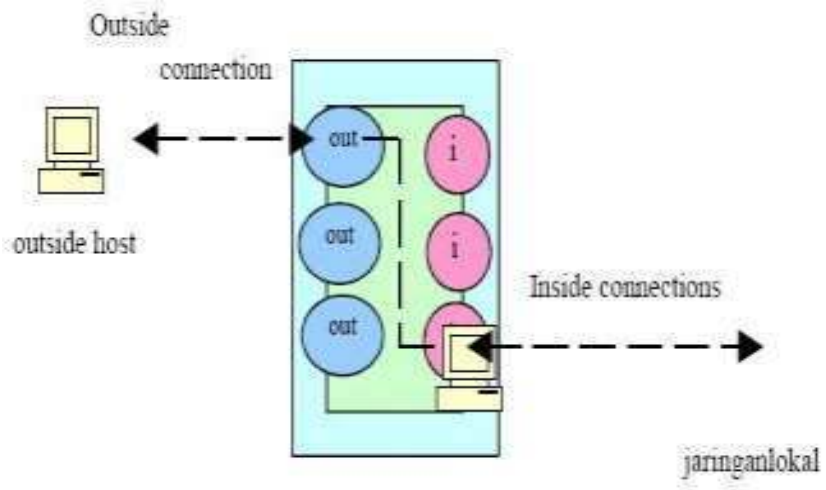
Sumber : Artikel Internet (Ammar- Firewall)

Merencanakan Jaringan Dengan Fireawll

Perencanaan sistem firewall di jaringan Anda terkait erat dengan jenis fasilitas yang tersedia bagi pengguna, toleransi risiko keamanan, waktu yang tersedia, biaya, dan keahlian (faktor teknis dan ekonomi).). Firewall biasanya terdiri dari area filter (juga dikenal sebagai layar atau choke) dan area gateway. Filter digunakan untuk membatasi akses, mempersempit saluran, atau memblokir kelas lalu lintas tertentu. Terjadinya akses berarti bahwa fungsi jaringan terbatas. Dua metode biasanya dicapai untuk mempertahankan kemampuan komunikasi jaringan di lingkungan firewall.:

1. Pertama, bayangkan bahwa jaringan kita berada di bawah perlindungan benteng, komunikasi dapat dilakukan melalui pintu keluar benteng. Teknik ini, yang disebut pemfilteran paket, hanya digunakan untuk menolak lalu lintas pada saluran atau saluran yang tidak digunakan dengan risiko keamanan yang signifikan dan mengizinkan lalu lintas di saluran lain. Berbagai pedoman dapat diterapkan saat melakukan operasi penyaringan paket. Pada dasarnya, ini menggunakan beberapa parameter yang tercantum dalam header paket data (arah (masuk atau keluar), alamat sumber dan tujuan, port sumber dan tujuan, dan) ke jaringan internal Mekanisme kontrol data yang memungkinkan aliran data ke dan dari . Jenis protokol transportasi. Router menampilkan informasi ini pada setiap paket data yang dilaluinya dan memutuskan apa yang harus dilakukan dengan paket tersebut berdasarkan jumlah aturan/program penyaringan paket. Ini menambahkan beberapa kebijakan keamanan jaringan ke keputusan perutean dasar perute. Tabel berikut menunjukkan contoh konfigurasi operasi pemfilteran paket untuk hanya menyediakan fungsionalitas SMTP masuk dan keluar di jaringan Anda.

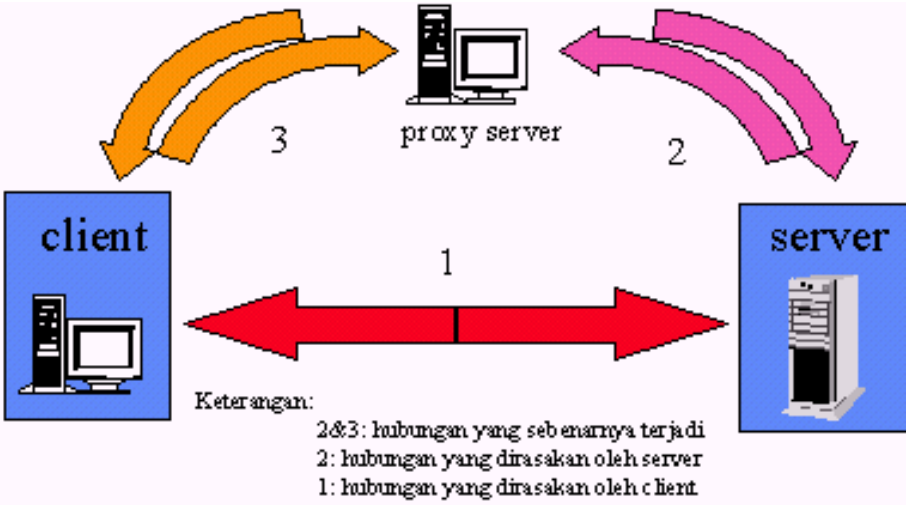
ISSN 1907-9044 (Print)
ISSN 2614-882X (Online)



Sumber : http://www.klik- kanan.com/fokus/firewall4.shtml

1. Aturan A dan B melayani koneksi SMTP (surat keluar) masuk, dan aturan C dan D melayani koneksi SMTP (surat keluar) keluar. Jika aturan sebelumnya gagal, aturan E adalah aturan default. Jika Anda perhatikan dengan seksama, dalam konfigurasi ini Anda memiliki lebih dari 1023 port (Aturan B dan D), yaitu lalu lintas SMTP dan koneksi masuk dan keluar pada program server seperti X11 (Port 6000), OpenWindows (Port 2000), atau sebagian besar database. Diizinkan. Program untuk menghubungi dari luar (Sybase, Oracle, Informix, dll.). Parameter penilaian penting lainnya, seperti penilaian asal, digunakan untuk mengesampingkan kemungkinan ini. Jadi, satu-satunya cara untuk melewati firewall adalah dengan menggunakan port SMTP. Jika Anda masih ragu dengan kejujuran pengguna port ini, Anda dapat melakukan analisis lebih lanjut terhadap informasi ACK..
2. Opsi kedua untuk menggunakan sistem proxy. Dalam hal ini, semua komunikasi antara dua jaringan harus dilakukan melalui operator (dalam hal ini server proxy). Beberapa protokol, seperti Telnet dan SMTP (Simple Mail Transport Protocol), ditangani lebih efektif oleh packet filtering, tetapi yang lain seperti File Transfer Protocol (FTP), Archie, Gopher, dan HyperText Transport Protocol (HTTP).Protokol diproses . Lebih efisien. Secara efektif menangani sistem proxy. Sebagian besar firewall menggunakan kombinasi dari kedua teknik ini (penyaringan paket dan proxy).
3. Metode kedua, menggunakan sistem proxy . Dalam sistem ini, semua komunikasi antara dua jaringan harus dilakukan melalui operator (dalam hal ini server proxy). Beberapa protokol, seperti telnet dan SMTP (Simple Mail Transport Protocol), ditangani lebih efektif oleh packet filtering, tetapi FTP (File Transfer Protocol), Archie, Gopher, HTTP (HyperText Transport Protocol), dll. Protokol lainnya adalah diproses lebih efektif menggunakan proxy. sistem. Sebagian besar firewall menggunakan kombinasi dari kedua teknik ini (penyaringan paket dan proxy). Dalam jaringan yang menerapkan sistem proxy, tautan komunikasi ke Internet diimplementasikan melalui sistem delegasi. Komputer yang dikenal oleh Internet bertindak sebagai "perwakilan" dari mesin lain yang ingin terhubung ke dunia luar. Protokol (set) server proxy tertentu beroperasi pada host rumah ganda atau host benteng dan dapat berkomunikasi dengan semua pengguna jaringan. Dalam hal ini, server proksi ini bertindak sebagai delegasi. Artinya, setiap program klien merujuk server proxy, yang terhubung ke server sebenarnya di Internet. Server proxy mengevaluasi semua permintaan koneksi dari klien dan menentukan mana yang diizinkan dan mana yang tidak diizinkan. Jika permintaan koneksi ini disetujui, server proxy meneruskan permintaan ke server sebenarnya.

ISSN 1907-9044 (Print)
ISSN 2614-882X (Online)



Sumber : http://www.klik- kanan.com/fokus/firewall4.shtml

Ada beberapa istilah yang mengacu pada berbagai jenis proxy, seperti proxy tingkat aplikasi, proxy tingkat rantai, proxy generik atau kustom, dan proxy pintar. Terlepas dari jenis proxy yang Anda gunakan, sistem ini memiliki beberapa implikasi.

a. Akses biasanya memerlukan klien dan prosedur yang berbeda, dan Anda perlu menyediakan server program untuk setiap aplikasi.
b. Sistem proxy memungkinkan Anda untuk menggunakan alamat IP pribadi Anda untuk jaringan internal Anda. Alamat IP kelas A (10.x.x.x) dapat digunakan untuk alamat IP pribadi yang digunakan dalam jaringan Internet. Memungkinkan komputer yang dapat terhubung ke jaringan internal mencapai jutaan komputer.
c. Paket SOCKS atau TIS-FWTK adalah contoh paket perangkat lunak proxy yang sering digunakan di Internet dan tersedia secara gratis.

Metode Penelitian

Metode penelitian yang digunakan dalam penulisan jurnal ini adalah dengan menggunakan studi pustaka. Dengan cara ini, penulis mengumpulkan berbagai informasi tentang topik artikel jurnal ini.

Pembahasan

Ada beberapa hal yang perlu diingat ketika mengoptimalkan firewall Anda. Pertama, Anda perlu menentukan kebijakan atau kebijakan firewall. Suatu kebijakan atau policy sangat penting sehingga kualitas firewall sangat ditentukan oleh kebijakan atau policy yang diterapkan. Definisi kebijakan meliputi: Putuskan apa yang perlu Anda tawarkan. Ini berarti bahwa itu adalah subjek dari pedoman yang akan kita buat.

a. Identifikasi individu atau kelompok yang tercakup dalam kebijakan
b. Gunakan jaringan untuk menentukan layanan yang dibutuhkan setiap individu atau kelompok.
c. Berdasarkan penggunaannya masing-masing oleh individu atau kelompok, bagaimana membuat konfigurasi layanan yang optimal lebih nyaman ditentukan.
d. Implementasi semua pedoman.

Anda kemudian dapat mengurai daftar port yang digunakan oleh berbagai protokol dan membuka port tersebut untuk firewall Anda. Portnya harus benar. Server web biasanya diidentifikasi melalui port 80, FTP (File Transfer Protocol) melalui port 21, dan SSH melalui port 22. Port ini menentukan port yang akan dibuka di sisi server web. Pada PC Anda, Anda perlu

membuka port untuk membuat koneksi keluar. Setting ini biasanya dilakukan secara otomatis oleh firewall ketika Anda menjalankan program yang membutuhkan koneksi internet. Setelah Anda mengetahui port yang dibutuhkan program Anda, buka port ini di firewall Anda.

Firewall modern secara otomatis mengenali jaringan Anda dan mengonfigurasinya sendiri. Kebanyakan firewall saat ini menyediakan pengaturan otomatis untuk kemampuan berbagi file dan printer. Firewall lain, seperti firewall XP, harus dikonfigurasi secara manual setiap kali. Untuk mengaktifkan berbagi file dan printer, buka port TCP 139 dan 445 serta port UDP 137 dan 138 untuk data yang masuk. Selain itu, Anda perlu meminta gema ICMP. Jika Anda terhubung ke Internet melalui router Anda, router Anda memiliki penjaga keamanan. Setting router yang perlu diubah adalah fungsi port forwarding. Sebagian besar router biasanya menonaktifkan fitur penerusan port secara default, jadi Anda harus mengaktifkannya. Ketika dikonfigurasi dengan benar, router menolak paket IP yang berisi pengirim palsu. Optimalisasi firewall selanjutnya adalah menentukan konfigurasi firewall yang benar. Ada beberapa konfigurasi firewall.

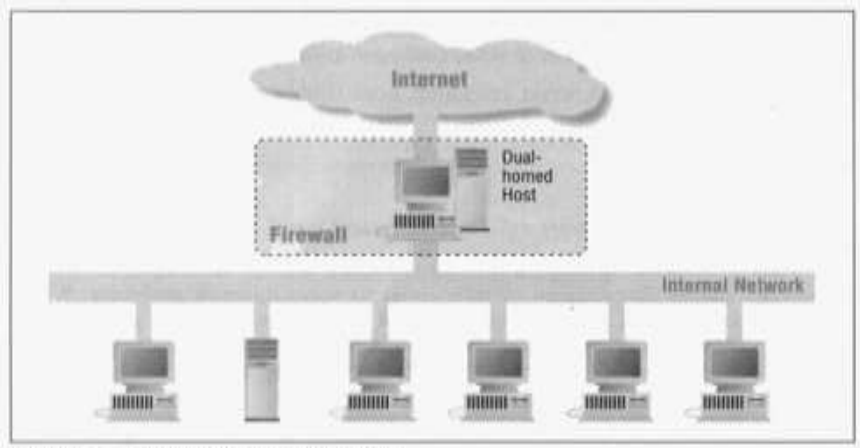


Figure 4–3. Dual-homed host architecture

Sumber : http://library.adisanggoro.or.id/Security/Transparan Digisec-5firewall.htm

1. Dual-homed host
   Host rumah ganda dapat menjadi router, tetapi karena merupakan firewall, arsitektur ini sepenuhnya memblokir lalu lintas IP. Oleh karena itu, jika paket dikirim, harus melalui proxy.

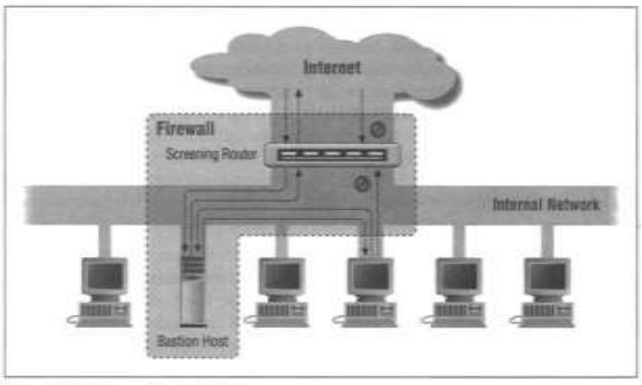


Figure 4–4. Screened host architecture

Sumber http://library.adisanggoro.or.id/Security/TransparanDigisec-5firewall.htm

2. Screened Host

Menggunakan bastion host yang terletak di intranet, semua komunikasi masuk dan keluar harus melalui proxy di dalam benteng dan kemudian melalui router filter. Bastion host adalah sistem/bagian yang dianggap administrator paling kuat dalam sistem keamanan jaringan. Sepintas, arsitektur dual-homed mungkin tampak lebih aman, tetapi pada kenyataannya, banyak kegagalan sistem dalam arsitektur dual-homed menyebabkan paket-paket dilewatkan dari satu sisi ke sisi lain. Oleh karena itu, alasan utama menggunakan arsitektur host yang difilter adalah untuk memudahkan router menggunakan komputer/host. Kelemahan utama dari keduanya adalah bahwa mereka memiliki "satu titik kegagalan".

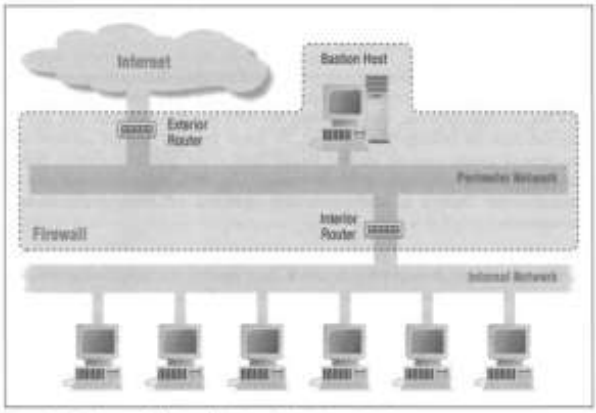


Figure 4-5. Screened subnet architecture (using two routers)

Sumber : http://library.adisanggoro.or.id/Security/Ir ansparanDigisec-5firewall.htm

3. Screened Subnet

Mengapa bastion host sering menjadi sasaran serangan. Idenya adalah jika bastion host disusupi, penyerang tidak akan dapat membobol jaringan internal. Oleh karena itu, bastion host terletak di batas jaringan. Untuk membobol jaringan, peretas perlu menyerang router eksternal dan internal. Ada juga batasan efektif di mana persyaratan sistem pertahanan harus berbeda untuk setiap lapisan. Jaringan batas. Artinya, jika seseorang berhasil membobol di luar router dan benteng, penyerang hanya dapat melihat paket yang tersimpan di jaringan perimeter. Akibatnya, lalu lintas komunikasi di jaringan internal (relatif sensitif) tidak terlihat oleh penyerang dari jaringan perimeter. Host bastion bertindak sebagai titik masuk untuk koneksi eksternal seperti SMTP, FTP, dan DNS. Sementara itu, Anda dapat terhubung ke server dari klien di Internet dengan dua cara:

a. Router memungkinkan klien untuk terhubung langsung ke server internet. Gunakan server proxy di benteng.
b. Bagian dalam router melindungi jaringan internal dari Internet dan jaringan perimeter.

Lalu lintas antara benteng dan pelanggan hanya diperbolehkan untuk hal-hal yang penting. Misalnya, koneksi SMTP antara benteng dan server email internal. Jika benteng berhasil dimanipulasi oleh hacker, itu akan menjadi target serangan, jadi perhatikan server komputer internal mana yang terhubung ke benteng. Pada kenyataannya, router eksternal memungkinkan banyak paket keluar dan menyaring hanya sejumlah kecil paket masuk. Namun, pengaturan untuk penyaringan jaringan internal biasanya sama untuk router internal dan eksternal. Peran utama router eksternal adalah memblokir paket dengan alamat palsu dari luar (untuk mencoba alamat IP salah satu host di jaringan internal). Karena harus dari internet. Mengapa bukan router internal? Ini sedikit lebih dapat diandalkan karena masih bisa dari batas bersih.

Kesimpulan

Keamanan merupakan hal yang sangat penting dalam dunia internet. Keamanan komputer dan jaringan penuh dengan ancaman, baik internal maupun eksternal. Firewall merupakan salah satu solusi untuk mengatasi keamanan ini. Dengan konfigurasi firewall yang tepat, kemampuan untuk mencatat data atau komputer di jaringan Anda jauh lebih aman. Konfigurasi firewall yang pertama adalah policy atau kebijakan firewall untuk apa yang menjadi subjek dari kebijakan tersebut, para pengguna yang menjadi subjek dari kebijakan tersebut, dan layanan yang dibutuhkan oleh masing-masing individu. Kemudian tentukan port yang digunakan oleh berbagai protokol, buka port tersebut ke firewall, dan buka port yang digunakan untuk berbagi file dan permintaan ping.

Selanjutnya, Anda perlu menentukan konfigurasi yang sesuai tergantung pada keadaan jaringan Anda. Subnet terlindung adalah konfigurasi dengan tingkat keamanan tertinggi. Dalam konfigurasi ini, dua router filter paket digunakan, sehingga jaringan lokal tidak terlihat dan perutean ke Internet tidak dapat dibuat atau Internet tidak terlihat dari luar. Router membuat koneksi. Antara internet dan bastion host, namun bukan berarti jaringan lokal tidak bisa terkoneksi dengan internet.

Dengan konfigurasi ini, firewall bisa lebih aman dan jauh lebih baik terhadap ancaman Internet. Namun, jaringan mungkin sedang diserang oleh peretas yang menjadi sasaran serangan tersebut. Tapi lebih baik ditutupi sedikit daripada tidak sama sekali.

Daftar Pustaka

Tanembaum, Andrew S. 1996. *Jaringan Komputer Edisi Bahasa Indonesia Jilid 1.*Prenhallindo : Jakarta.

Majalah CHIP edisi Mei 2007. *Firewall Yang Sempurna.*

http://www.erlangga.co.id/blog/viewtopic.
php?t=188&sid=f9320f1898d08eba9948454883072f1b

http://students.ukdw.ac.id/~22022807/kommasd.html

http://library.adisanggoro.or.id/Security/Tr ansparanDigisec-5firewall.htm

http://www.klik- kanan.com/fokus/firewall.shtml

http://www.ictwatch.com/internetsehat/do wnload/internetsehatmodulemanual/ modul_personalfirewall.pdf http://www.ictwatch.com/internetsehat/do wnload/internetsehatmodulemanual/ modul_personalfirewall.pdf http://ilmukomputer.com