PENGERTIAN FUNGSI, MANFAAT DAN CARA KERJA FIREWALL

Allex Sandra Willyan

allexsandrawillyan@gmail.com

Abstrak

Artikel ini berisi tentang pengertian fungsi, manfaat dan cara kerja firewall, artikel ini bisa mempermudah teman-teman dalam mengetahui tentang firewall , semoga artikel ini dapat membantu dan bermanfaat untuk rekan-rekan yang ingin mengetahui apa itu firewall, Terimakasih.

Kata Kunci: fungsi firewall,cara kerja firewall, manfaat firewall

Pendahuluan

Pengertian Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar.

Pembahasan

Pengertian Firewall yang dimaksudkan diatas adalah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadapa jaringan yang dianggap tidak aman. Fire-wall dapat berupa perangkat lunak (program komputer atau aplikasi) atau perangkat keras (peralatan khusus untuk menjalankan program fire-wall) perangkat yang menyaring lalu lintas jaringan antara jaringan. Perlindungan Firewall diperlukan untuk komputasi perangkat seperti komputer yang diaktifkan dengan koneksi Internet. Meningkatkan tingkat keamanan jaringan komputer dengan memberikan informasi rinci tentang pola-pola lalu lintas jaringan. Perangkat ini penting dan sangat diperlukan karena bertindak sebagai gerbang keamanan antara jaring komputer internal dan jaringan komputer eksternal.

Secara umum Firewall digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar. Saat ini, pengertian firewall difahami dengan istilah generik yang merujuk pada fungsi firewall sebagai sistem pengatur komunikasi antar dua jaringan yang berlainan. Mengingat sekarang ini banyak perusahaan yang memiliki akses ke Internet maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, sehingga fungsi fire-wall menjadi hal yang sangat esensial."

Fungsi Firewall

Sebelum memahami fungsi firewall mari kita fahami atribut pentingnya sbb:

- Semua jaringan komunikasi melewati fire wall
- Hanya lalu lintas resmi diperbolehkan oleh fire wall
- Memiliki kemampuan untuk menahan serangan Internet

Fungsi firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi Firewal mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi, beberapa kriteria yang dilakukan fire-wall apakah memperbolehkan paket data lewati atau tidak, antara lain :

- Alamat IP dari komputer sumber
- Port TCP/UDP sumber dari sumber.
- Alamat IP dari komputer tujuan.
- Port TCP/UDP tujuan data pada komputer tujuan

Informasi dari header yang disimpan dalam paket data.

Fungsi Firewall melakukan autentifikasi terhadap akses kejaringan. Applikasi proxy Fire-wall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntutnya untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

Manfaat Firewall

Manfaat firewalluntuk menjaga informasi rahasia dan berharga yang menyelinap keluar tanpa sepengetahuan. Sebagai contoh, FTP (File Transfer Protocol) lalu lintas dari jaringan komputer organisasi dikendalikan oleh fire-wall. Hal ini dilakukan untuk mencegah pengguna di jaringan mengirim file rahasia yang disengaja atau tidak sengaja kepada pihak lain.

Manfaat Firewallsebagai filter juga digunakan untuk mencegah lalu lintas tertentu mengalir ke subnet jaringan. Hal ini mencegah pengguna berbagi file, dan bermain-main di jaringan.Aplikasi jenis ini berguna terutama dalam sektor korporasi.

Manfaat firewalllainnya adalah untuk memodifikasi paket data yang datang di fire-wall. Proses ini disebut Network Address Translation (NAT). Ada jenis NAT disebut NAT dasar, di mana alamat IP (Internet Protocol) pribadi dari jaringan komputer yang tersembunyi di balik satu alamat IP tertentu. Proses ini disebut sebagai IP samaran. Hal ini membantu pengguna dalam sebuah jaringan yang meliputi sistem tanpa nomor IP publik yang beralamat, untuk mengakses Internet.

Akurasi data seperti informasi keuangan, spesifikasi produk, harga produk dll, sangat penting bagi setiap perkembangan bisnis. Jika informasi tersebut diubah oleh sumber eksternal, maka akan memberikan dampak merugikan.Manfaat Firewall disini adalah mencegah modifikasi data yang tidak sah di website .

Jika sistem tidak tersedia bagi pengguna secara tepat waktu, maka halini akan menyebabkan penurunan produktivitas karyawan, kehilangan kepercayaan konsumen, dan publisitas yang buruk. Fire-wall memastikan ketersediaan sistem.

Cara Kerja Firewall

Komputer memiliki ribuan port yang dapat diakses untuk berbagai keperluan. Cara Kerja Firewall dari komputer adalah menutup port kecuali untuk beberapa port tertentu yang perlu tetap terbuka. Firewall di komputer bertindak sebagai garis pertahanan terdepan dalam mencegah semua jenis hacking ke dalam jaringan, karena, setiap hacker yang mencoba untuk menembus ke dalam jaringan komputer akan mencari port yang terbuka yang dapat diaksesnya.

Teknologi firewall saat ini sudah sangat canggih. Sebelumnya, cara kerja firewall dengan menyaring lalu lintas jaringan yang menggunakan alamat IP, nomor port, dan protokol, tapi saat ini fire-wall dapat menyaring data dengan mengidentifikasi pesan konten itu sendiri. Dengan bantuan fire-wall, informasi sensitif atau tidak layak dapat dicegah melalui interface. Pastikan sistem keamanan jaringan di lapisi firewall

Mengatur dan Mengontrol Lalu lintas jaringan

Fungsi pertama yang dapat dilakukan oleh firewall adalah firewall harus dapat mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi oleh firewall. Firewall melakukan hal yang demikian, dengan

melakukan inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan penapisan (filtering) terhadap koneksi berdasarkan hasil inspeksi paket dan koneksi tersebut.

Proses inspeksi Paket

Inspeksi paket (‘packet inspection) merupakan proses yang dilakukan oleh firewall untuk ‘menghadang’ dan memproses data dalam sebuah paket untuk menentukan bahwa paket tersebut diizinkan atau ditolak, berdasarkan kebijakan akses (access policy) yang diterapkan oleh seorang administrator. Firewall, sebelum menentukan keputusan apakah hendak menolak atau menerima komunikasi dari luar, ia harus melakukan inspeksi terhadap setiap paket (baik yang masuk ataupun yang keluar) di setiap antarmuka dan membandingkannya dengan daftar kebijakan akses. Inspeksi paket dapat dilakukan dengan melihat elemen-elemen berikut, ketika menentukan apakah hendak menolak atau menerima komunikasi:

1. Alamat IPdari komputer sumber
2. Portsumber pada komputer sumber
3. Alamat IPdari komputer tujuan
4. Porttujuan data pada komputer tujuan
5. Protokol IP
6. Informasi header-header yang disimpan dalam paket
7. Koneksi dan Keadaan Koneksi

Agar dua host TCP/IP dapat saling berkomunikasi, mereka harus saling membuat koneksi antara satu dengan lainnya. Koneksi ini memiliki dua tujuan:

Komputer dapat menggunakan koneksi tersebut untuk mengidentifikasikan dirinya kepada komputer lain, yang meyakinkan bahwa sistem lain yang tidak membuat koneksi tidak dapat mengirimkan data ke komputer tersebut. Firewall juga dapat menggunakan informasi koneksi untuk menentukan koneksi apa yang diizinkan oleh kebijakan akses dan menggunakannya untuk menentukan apakah paket data tersebut akan diterima atau ditolak.

Koneksi digunakan untuk menentukan bagaimana cara dua host tersebut akan berkomunikasi antara satu dengan yang lainnya(apakah dengan menggunakan koneksi connection-oriented, atau connectionless).

Ilustrasi mengenai percakapan antara dua buah host

Kedua tujuan tersebut dapat digunakan untuk menentukan keadaan koneksi antara dua host tersebut, seperti halnya cara manusia bercakap-cakap. Jika Amir bertanya kepada Aminah mengenai sesuatu, maka Aminah akan meresponsnya dengan jawaban yang sesuai dengan pertanyaan yang diajukan oleh Amir; Pada saat Amir melontarkan pertanyaannya kepada Aminah, keadaan percakapan tersebut adalah Amir menunggu respons dari Aminah. Komunikasi di jaringan juga mengikuti cara yang sama untuk memantau keadaan percakapan komunikasi yang terjadi.

Firewall dapat memantau informasi keadaan koneksi untuk menentukan apakah ia hendak mengizinkan lalu lintas jaringan. Umumnya hal ini dilakukan dengan memelihara sebuah tabel keadaan koneksi (dalam istilah firewall: state table) yang memantau keadaan semua komunikasi yang melewati firewall. Dengan memantau keadaan koneksi ini, firewall dapat menentukan apakah data yang melewati firewall sedang "ditunggu" oleh host yang dituju, dan jika ya, aka mengizinkannya. Jika data yang melewati firewall tidak cocok dengan keadaan koneksi yang didefinisikan oleh tabel keadaan koneksi, maka data tersebut akan ditolak. Hal ini umumnya disebut sebagai Stateful Inspection.

Stateful Packet Inspection

Ketika sebuah firewall menggabungkan stateful inspection dengan packet inspection, maka firewall tersebut dinamakan dengan Stateful Packet Inspection (SPI). SPI merupakan proses inspeksi paket yang tidak dilakukan dengan menggunakan struktur paket dan data yang terkandung dalam paket, tapi juga pada keadaan apa host-host yang saling berkomunikasi tersebut berada. SPI mengizinkan firewall untuk melakukan penapisan tidak hanya berdasarkan isi paket tersebut, tapi juga berdasarkan koneksi atau keadaan koneksi, sehingga dapat mengakibatkan firewall memiliki kemampuan yang lebih fleksibel, mudah diatur, dan memiliki skalabilitas dalam hal penapisan yang tinggi.

Salah satu keunggulan dari SPI dibandingkan dengan inspeksi paket biasa adalah bahwa ketika sebuah koneksi telah dikenali dan diizinkan (tentu saja setelah dilakukan inspeksi), umumnya sebuah kebijakan (policy) tidak dibutuhkan untuk mengizinkan komunikasi balasan karena firewall tahu respons apa yang diharapkan akan diterima. Hal ini memungkinkan inspeksi terhadap data dan perintah yang terkandung dalam sebuah paket data untuk menentukan apakah sebuah koneksi diizinkan atau tidak, lalu firewall akan secara otomatis memantau keadaan percakapan dan secara dinamis mengizinkan lalu lintas yang sesuai dengan keadaan. Ini merupakan peningkatan yang

cukup signifikan jika dibandingkan dengan firewall dengan inspeksi paket biasa. Apalagi, proses ini diselesaikan tanpa adanya kebutuhan untuk mendefinisikan sebuah kebijakan untuk mengizinkan respons dan komunikasi selanjutnya. Kebanyakan firewall modern telah mendukung fungsi ini.

Melakukan autentikasi terhadap akses

Fungsi fundamental firewall yang kedua adalah firewall dapat melakukan autentikasi terhadap akses.

Protokol TCP/IP dibangun dengan premis bahwa protokol tersebut mendukung komunikasi yang terbuka. Jika dua host saling mengetahui alamat IP satu sama lainnya, maka mereka diizinkan untuk saling berkomunikasi. Pada awal-awal perkembangan Internet, hal ini boleh dianggap sebagai suatu berkah. Tapi saat ini, di saat semakin banyak yang terhubung ke Internet, mungkin kita tidak mau siapa saja yang dapat berkomunikasi dengan sistem yang kita miliki. Karenanya, firewall dilengkapi dengan fungsi autentikasi dengan menggunakan beberapa mekanisme autentikasi, sebagai berikut:

Firewall dapat meminta input dari pengguna mengenai nama pengguna (user name) serta kata kunci (password). Metode ini sering disebut sebagai extended authentication atau xauth. Menggunakan xauth pengguna yang mencoba untuk membuat sebuah koneksi akan diminta input mengenai nama dan kata kuncinya sebelum akhirnya diizinkan oleh firewall. Umumnya, setelah koneksi diizinkan oleh kebijakan keamanan dalam firewall, firewall pun tidak perlu lagi mengisikan input password dan namanya, kecuali jika koneksi terputus dan pengguna mencoba menghubungkan dirinya kembali.

Metode kedua adalah dengan menggunakan sertifikat digitaldan kunci publik. Keunggulan metode ini dibandingkan dengan metode pertama adalah proses autentikasi dapat terjadi tanpa intervensi pengguna. Selain itu, metode ini lebih cepat dalam rangka melakukan proses autentikasi. Meskipun demikian, metode ini lebih rumit implementasinya karena membutuhkan banyak komponen seperti halnya implementasi infrastruktur kunci publik.

Metode selanjutnya adalah dengan menggunakan Pre-Shared Key (PSK) atau kunci yang telah diberitahu kepada pengguna. Jika dibandingkan dengan sertifikat digital, PSK lebih mudah diimplenentasikan karena lebih sederhana, tetapi PSK juga mengizinkan proses autentikasi terjadi tanpa intervensi pengguna. Dengan menggunakan PSK, setiap host akan diberikan sebuah kunci yang telah ditentukan

sebelumnya yang kemudian digunakan untuk proses autentikasi. Kelemahan metode ini adalah kunci PSK jarang sekali diperbarui dan banyak organisasi sering sekali menggunakan kunci yang sama untuk melakukan koneksi terhadap host-host yang berada pada jarak jauh, sehingga hal ini sama saja meruntuhkan proses autentikasi. Agar tercapai sebuah derajat keamanan yang tinggi, umumnya beberapa organisasi juga menggunakan gabungan antara metode PSK dengan xauth atau PSK dengan sertifikat digital.

Dengan mengimplementasikan proses autentikasi, firewall dapat menjamin bahwa koneksi dapat diizinkan atau tidak. Meskipun jika paket telah diizinkan dengan menggunakan inspeksi paket (PI) atau berdasarkan keadaan koneksi (SPI), jika host tersebut tidak lolos proses autentikasi, paket tersebut akan dibuang.

Melindungi sumber daya dalam jaringan privat

Salah satu tugas firewall adalah melindungi sumber daya dari ancaman yang mungkin datang. Proteksi ini dapat diperoleh dengan menggunakan beberapa pengaturan peraturan akses (access control), penggunaan SPI, application proxy, atau kombinasi dari semuanya untuk mengamankan host yang dilindungi supaya tidak dapat diakses oleh host-host yang mencurigakan atau dari lalu lintas jaringan yang mencurigakan. Meskipun demikian, firewall bukan satu-satunya metode proteksi teraman terhadap sumber daya, dan mempercayakan proteksi firewall dari ancaman secara eksklusif adalah salah satu kesalahan fatal.

Jika sebuah host yang menjalankan sistem operasi tertentu yang memiliki lubang keamanan yang belum ditambal dikoneksikan ke Internet, firewall mungkin tidak dapat mencegah dieksploitasinya host tersebut oleh host-host lainnya, khususnya jika exploit tersebut menggunakan lalu lintas yang oleh firewall telah diizinkan (dalam konfigurasinya). Sebagai contoh, jika sebuah packet-inspection firewall mengizinkan lalu lintas HTTP ke sebuah web server yang menjalankan sebuah layanan web yang memiliki lubang keamanan yang belum ditambal, maka seorang pengguna yang “iseng” dapat saja membuat exploit untuk meruntuhkan web server tersebut karena memang web server yang bersangkutan memiliki lubang keamanan yang belum ditambal.

Dalam contoh ini, web server tersebut akhirnya mengakibatkan proteksi yang ditawarkan oleh firewall menjadi tidak berguna. Hal ini disebabkan oleh firewall tidak dapat membedakan antara request HTTP yang mencurigakan atau tidak. Apalagi, jika firewall yang digunakan bukan application proxy. Oleh karena itulah, sumber daya yang

dilindungi haruslah dipelihara dengan melakukan penambalan terhadap lubang-lubang keamanan, selain tentunya dilindungi oleh firewall.

Cara Kerja Firewall

Firewall berada di antara kedua jaringan seperti internet dan komputer sehingga firewall berfungsi sebagai pelindung. Tujuan utama adanya firewall adalah untuk user yang tidak menginginkan lalu lintas jaringan yang berusaha masuk ke komputer, namun tidak hanya itu saja yang bisa dilakukan firewall. Firewall juga dapat menganalisis jaringan yang mencoba masuk ke komputer anda, dan dapat melakukan apa yang harus dilakukan ketika jaringan tersebut masuk. Contohnya saja, firewall bisa diatur untuk memblokir beberapa jenis jaringan yang mencoba keluar atau mencatat log lalu lintas jaringan yang mencurigakan.

Firewall bisa memiliki berbagai aturan yang dapat anda tambahkan atau hapus untuk menolak jaringan tertentu. Contohnya saja, hanya dapat mengakses alamat IP tertentu atau mengumpulkan semua akses dari tempat lain untuk ke satu tempat yang aman terlebih dahulu

Packet-Filter Firewall

Contoh pengaturan akses (access control) yang diterapkan dalam firewall

Pada bentuknya yang paling sederhana, sebuah firewall adalah sebuah router atau komputer yang dilengkapi dengan dua buah NIC (Network Interface Card, kartu antarmuka jaringan) yang mampu melakukan penapisan atau penyaringan terhadap paket-paket yang masuk. Perangkat jenis ini umumnya disebut dengan packet-filtering router.

Firewall jenis ini bekerja dengan cara membandingkan alamat sumber dari paket-paket tersebut dengan kebijakan pengontrolan akses yang terdaftar dalam Access Control List firewall, router tersebut akan mencoba memutuskan apakah hendak meneruskan paket yang masuk tersebut ke tujuannya atau menghentikannya. Pada bentuk yang lebih sederhana lagi, firewall hanya melakukan pengujian terhadap alamat IP atau nama domain yang menjadi sumber paket dan akan menentukan apakah hendak meneruskan atau menolak paket tersebut. Meskipun demikian, packet-filtering router tidak dapat digunakan untuk memberikan akses (atau menolaknya) dengan menggunakan basis hak-hak yang dimiliki oleh pengguna.

Cara kerja packet filter firewall

Packet-filtering router juga dapat dikonfigurasikan agar menghentikan beberapa jenis lalu lintas jaringan dan tentu saja mengizinkannya. Umumnya, hal ini dilakukan dengan mengaktifkan/menonaktifkan port TCP/IP dalam sistem firewall tersebut. Sebagai contoh, port 25 yang digunakan oleh Protokol SMTP (Simple Mail Transfer Protocol) umumnya dibiarkan terbuka oleh beberapa firewall untuk mengizinkan surat elektronik dari Internet masuk ke dalam jaringan privat, sementara port lainnya seperti port 23 yang digunakan oleh Protokol Telnet dapat dinonaktifkan untuk mencegah pengguna Internet untuk mengakses layanan yang terdapat dalam jaringan privat tersebut. Firewall juga dapat memberikan semacam pengecualian (exception) agar beberapa aplikasi dapat melewati firewall tersebut. Dengan menggunakan pendekatan ini, keamanan akan lebih kuat tapi memiliki kelemahan yang signifikan yakni kerumitan konfigurasi terhadap firewall: daftar Access Control List firewall akan membesar seiring dengan banyaknya alamat IP, nama domain, atau port yang dimasukkan ke dalamnya, selain tentunya juga exception yang diberlakukan.

Circuit Level Gateway

Cara kerja circuit level firewall

Firewall jenis lainnya adalah Circuit-Level Gateway, yang umumnya berupa komponen dalam sebuah proxy server. Firewall jenis ini beroperasi pada level yang lebih tinggi dalam model referensi tujuh lapis OSI (bekerja pada lapisan sesi/session layer) daripada Packet Filter Firewall. Modifikasi ini membuat firewall jenis ini berguna dalam rangka menyembunyikan informasi mengenai jaringan terproteksi, meskipun firewall ini tidak melakukan penyaringan terhadap paket-paket individual yang mengalir dalam koneksi.

Dengan menggunakan firewall jenis ini, koneksi yang terjadi antara pengguna dan jaringan pun disembunyikan dari pengguna. Pengguna akan dihadapkan secara langsung dengan firewall pada saat proses pembuatan koneksi dan firewall pun akan membentuk koneksi dengan sumber daya jaringan yang hendak diakses oleh pengguna setelah mengubah alamat IP dari paket yang ditransmisikan oleh dua belah pihak. Hal ini mengakibatkan terjadinya sebuah sirkuit virtual (virtual circuit) antara pengguna dan sumber daya jaringan yang ia akses.

Firewall ini dianggap lebih aman dibandingkan dengan Packet-Filtering Firewall, karena pengguna eksternal tidak dapat melihat alamat IP jaringan internal dalam paket-paket yang ia terima, melainkan alamat IP dari firewall.

Application Level Firewall

Application Level Firewall (disebut juga sebagaiapplication proxy atauapplication level gateway)

Firewall jenis lainnya adalah Application Level Gateway (atau Application-Level Firewall atau sering juga disebut sebagai Proxy Firewall), yang umumnya juga merupakan komponen dari sebuah proxy server. Firewall ini tidak mengizinkan paket yang datang untuk melewati firewall secara langsung. Tetapi, aplikasi proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.

Umumnya, firewall jenis ini akan melakukan autentikasi terlebih dahulu terhadap pengguna sebelum mengizinkan pengguna tersebut untuk mengakses jaringan. Selain itu, firewall ini juga mengimplementasikan mekanisme auditing dan pencatatan (logging) sebagai bagian dari kebijakan keamanan yang diterapkannya. Application Level Firewall juga umumnya mengharuskan beberapa konfigurasi yang diberlakukan pada pengguna untuk mengizinkan mesin klien agar dapat berfungsi. Sebagai contoh, jika sebuah proxy FTPdikonfigurasikan di atas sebuah application layer gateway, proxy tersebut dapat dikonfigurasikan untuk mengizinlan beberapa perintah FTP, dan menolak beberapa perintah lainnya. Jenis ini paling sering diimplementasikan pada proxy SMTP sehingga mereka dapat menerima surat elektronik dari luar (tanpa menampakkan alamat e-mail internal), lalu meneruskan e-mail tersebut kepada e-mail server dalam jaringan. Tetapi, karena adanya pemrosesan yang lebih rumit, firewall jenis ini mengharuskan komputer yang dikonfigurasikan sebagai application gateway memiliki spesifikasi yang tinggi, dan tentu saja jauh lebih lambat dibandingkan dengan packet-filter firewall.

NAT Firewall

NAT (Network Address Translation) Firewall secara otomatis menyediakan proteksi terhadap sistem yang berada di balik firewall karena NAT Firewall hanya mengizinkan koneksi yang datang dari komputer-komputer yang berada di balik firewall. Tujuan dari NAT adalah untuk melakukan multiplexing terhadap lalu lintas dari jaringan internal untuk kemudian menyampaikannya kepada jaringan yang lebih luas (MAN, WAN atau

Internet) seolah-olah paket tersebut datang dari sebuah alamat IP atau beberapa alamat IP. NAT Firewall membuat tabel dalam memori yang mengandung informasi mengenai koneksi yang dilihat oleh firewall. Tabel ini akan memetakan alamat jaringan internal ke alamat eksternal. Kemampuan untuk menaruh keseluruhan jaringan di belakang sebuah alamat IP didasarkan terhadap pemetaan terhadap port-port dalam NAT firewall.

Stateful Firewall

Cara kerja stateful firewall

Stateful Firewall merupakan sebuah firewall yang menggabungkan keunggulan yang ditawarkan oleh packet-filtering firewall, NAT Firewall, Circuit-Level Firewall dan Proxy Firewall dalam satu sistem. Stateful Firewall dapat melakukan filtering terhadap lalu lintas berdasarkan karakteristik paket, seperti halnya packet-filtering firewall, dan juga memiliki pengecekan terhadap sesi koneksi untuk meyakinkan bahwa sesi koneksi yang terbentuk tersebut diizinlan. Tidak seperti Proxy Firewall atau Circuit Level Firewall, Stateful Firewall umumnya didesain agar lebih transparan (seperti halnya packet-filtering firewall atau NAT firewall). Tetapi, stateful firewall juga mencakup beberapa aspek yang dimiliki oleh application level firewall, sebab ia juga melakukan inspeksi terhadap data yang datang dari lapisan aplikasi (application layer) dengan menggunakan layanan tertentu. Firewall ini hanya tersedia pada beberapa firewall kelas atas, semacam Cisco PIX. Karena menggabungkan keunggulan jenis-jenis firewall lainnya, stateful firewall menjadi lebih kompleks.

Virtual Firewall

Virtual Firewall adalah sebutan untuk beberapa firewall logis yang berada dalam sebuah perangkat fisik (komputer atau perangkat firewall lainnya). Pengaturan ini mengizinkan beberapa jaringan agar dapat diproteksi oleh sebuah firewall yang unik yang menjalankan kebijakan keamanan yang juga unik, cukup dengan menggunakan satu buah perangkat. Dengan menggunakan firewall jenis ini, sebuah ISP (Internet Service Provider) dapat menyediakan layanan firewall kepada para pelanggannya, sehingga mengamankan lalu lintas jaringan mereka, hanya dengan menggunakan satu buah perangkat. Hal ini jelas merupakan penghematan biaya yang signifikan, meski firewall jenis ini hanya tersedia pada firewall kelas atas, seperti Cisco PIX 535.

Transparent Firewall

Transparent Firewall (juga dikenal sebagai bridging firewall) bukanlah sebuah firewall yang murni, tetapi ia hanya berupa turunan dari stateful Firewall. Daripada firewall-firewall lainnya yang beroperasi pada lapisan IP ke atas, transparent firewall bekerja pada lapisan Data-Link Layer, dan kemudian ia memantau lapisan-lapisan yang ada di atasnya. Selain itu, transparent firewall juga dapat melakukan apa yang dapat dilakukan oleh packet-filtering firewall, seperti halnya stateful firewall dan tidak terlihat oleh pengguna (karena itulah, ia disebut sebagai Transparent Firewall).

Intinya, transparent firewall bekerja sebagai sebuah bridge yang bertugas untuk menyaring lalu lintas jaringan antara dua segmen jaringan. Dengan menggunakan transparent firewall, keamanan sebuah segmen jaringan pun dapat diperkuat, tanpa harus mengaplikasikan NAT Filter. Transparent Firewall menawarkan tiga buah keuntungan, yakni sebagai berikut:

Konfigurasi yang mudah (bahkan beberapa produk mengklaim sebagai "Zero Configuration"). Hal ini memang karena transparent firewall dihubungkan secara langsung dengan jaringan yang hendak diproteksinya, dengan memodifikasi sedikit atau tanpa memodifikasi konfigurasi firewall tersebut. Karena ia bekerja pada data-link layer, pengubahan alamat IP pun tidak dibutuhkan. Firewall juga dapat dikonfigurasikan untuk melakukan segmentasi terhadap sebuah subnet jaringan antara jaringan yang memiliki keamanan yang rendah dan keamanan yang tinggi atau dapat juga untuk melindungi sebuah host, jika memang diperlukan.

Kinerja yang tinggi. Hal ini disebabkan oleh firewall yang berjalan dalam lapisan data-link lebih sederhana dibandingkan dengan firewall yang berjalan dalam lapisan yang lebih tinggi. Karena bekerja lebih sederhana, maka kebutuhan pemrosesan pun lebih kecil dibandingkan dengan firewall yang berjalan pada lapisan yang tinggi, dan akhirnya performa yang ditunjukannya pun lebih tinggi.

Tidak terlihat oleh pengguna (stealth). Hal ini memang dikarenakan Transparent Firewall bekerja pada lapisan data-link, dan tidak membutuhkan alamat IP yang ditetapkan untuknya (kecuali untuk melakukan manajemen terhadapnya, jika memang jenisnya managed firewall). Karena itulah, transparent firewall tidak dapat terlihat oleh para penyerang. Karena tidak dapat diraih oleh penyerang (tidak memiliki alamat IP), penyerang pun tidak dapat menyerangnya.

Hybrid Firewalls

Firewall jenis ini menggunakan elemen-elemen dari satu atau lebih tipe firewall. Hybrid firewall sebenarnya bukan sesuatu yang baru. Firewall komersil yang pertama, DEC SEAL, adalah firewall berjenis hybrid, dengan menggunakan proxy pada sebuah bastion hosts (mesin yang dilabeli sebagai gatekeeper pada) dan packet filtering pada gateway (gate). Kita bisa saja menambahkan sebuah circuit gateway atau packet filtering pada firewall berjenis application gateway, karena untuk itu hanya diperlukan kode proxy yang baru yang ditulis untuk setiap service baru yang akan disediakan. Kita juga dapat memberikan autentifikasi pengguna yang lebih ketat pada Stateful Packet Filter dengan menambahkan proxy untuk tiap service.

Penutup

Semoga artikel yang saya buat dapat membantu dan mempermudah teman-teman dalam memahami tentang pengertian fungsi, manfaat dan cara kerja firewall.

Terimakasih.

Referensi

http://www.ilmu-komputer.id

http://www.patartambunan.com

http://www.firewallindonesia.com

http://www.cepatbelajar.com

http://www.wikipedia.id

Biografi

Allex Sandra Willyan, Tanggal lahir 6 juni 1994 . Sedang melanjutkan pendidikan disalah satu perguruan tinggi di kota tangerang,