1. Pengertian Firewall

Firewalll merupakan kombinasi perangkat kuras dan perangkat lunak yang dirancang untuk melakukan pemeriksaan terhadap aliran lalu lintas dari jaringan yang ada dan setiap permintaan yang terhubung pada jaringan. Firewall merupakan sitem proteksi yang digunakan untuk melakukan pengawasan setiap lalu lintas atau paket data yang menuju atau meninggalkan suatu jaringan. Setiap paket data tersebut melalui proses pemeriksaan kemudian diterima dengan baik atau terhindar dari berbagai ancaman ketika proses transfer pada system jaringan.

Fungsi dari firewall adalah untuk mecegah keluar masuknya aliran paket data yang tidak memenuhi criteria keamanan. Selain itu Firewall dapat menjalankan program aplikasi dengan cara memfilter informasi yang melaluinya.

Firewall bekerja pada beberapa lapisan jaringan Lapisan yang tertinggi yaitu bekerja pada lapisan aplikasi dan lapisan terendah pada lapisan data-link.

Tujuan utama firewall adalah :

1. Menjaga akses ( proses masuk atau keluar ) pada suatu system dari orang yang tidak bertanggung jawab atau orang yang tidak berwenang.
2. Memeriksa aliran lalu lintas jaringan pada setiap lokaso berdasarkan paket data sesuai dengan criteria yang ada.
3. Meletakkan Firewall

Firewall sebaiknya diletakkan sebelum perangkat jaringan seperti router, switch, dan server data.

1. Karakteristik Firewall

Firewall mempunyai karakteristik sebgai berikut :

1. Semua hubugan atau setiap kegiatan yang terhubung dengan system jaringan, baik proses masuk maupun keluarnya informasi / paket data harus melewati firewall yang telah terpasang.
2. Untuk dapat melewati firewall yang terpasang pada suatu system jaringan, suatu kegiatan harus terdaftar atau dikenali oleh firewall dengan pengaturan policy pada konfigurasi keamanan local.
3. Firewall yang tanggung adalah firewall yang mampu, kebal, dan kuat terhadap sumua serangan yang ada pada suatu system jaringan.
4. Jenis Firewall

Firewall dapat dibedakan menjadi beberapa jenis diantaranya sebagai berikut :

1. Packet Filtering Router / Bridge

Merupakan jenis firewall yang mengatur semua paket IP, baik yang menuju, melewati, maupun akan dituju oleh peket tersebut. Firewall jenis ini didesain untuk melakukan pengontrolan terhadap paket, yaitu berdasarkan aliran paket, dilihat dari alamat asal, alamat tujuan, port, dan tipe informasi, serta paket yang yang dikandung dalam tiap paket.

Keuntungan menggunakan IP filtering firewall

1. Sangat aman, tetapi menghabiskan log yang penting.
2. Mudah untuk diimplementasikan.
3. Transparan untuk pemakai karena terlalu cepat.
4. Dapat menahan dan memblokir serangan berupa usaha mengakses jaringan.
5. Tidak dapat memberikan akses dari luar ke dalam jaringan private kepada seseorang tanpa memberikan akses kepada semua orang dari luar jaringan private.

Kelemahan menggunakan IP filtering firewall :

1. Konfigurasi kompleks, agak sulit dalam mengkonfigurasi karena penguasaan terhadap port, ipaddress,dll.
2. Mudahterja dikesalahan dalam konfigurasi.
3. Susah untuk mengkonfig pada protocol yang dinamis (misalnyaFTP)
4. Tidak dapat mengfilter berdasarkan content (misalnya lampiran pada email, javascript, ActiveX)

Jenis serangan yang terjadi pada firewall jenis tipe paket filtering adalah sebagai berikut :

1. IP addres spoofing merupakan jenis serangan dengan penyusup berasal dari luar yang menggunakn IP address jaringan local dengan the diizinkan melalui firewall.
2. Source routing attack merupakan jenis serangan yang tidak melakukan analisis terlebih dahulu terhadap informasi sumber IP sehingga dapat melakukan bypass firewall.
3. Tiny fragment attack merupakan jenis serangan yang dapat membagi-bagi IP ke dalam bagian yang lebih kecil. Jenis ini didesain untuk melakukan penipuan aturan penyaringan yang bergantung pada informasi dari TCP header.
4. Application Level Gateway

Merupakan jenis firewall yang berfungsi untuk memperkuat atau menyalurkan arus aplikasi dan sering dikenal dengan istilah proxy server.

Jenis firewall ini khusus dikonfigurasi untuk mendukung beberapa aplikasi yang benar-benar terdaftar pada aplikasi firewall saja dan melakukan penolakan aplikasi-aplikasi lainnya untuk melewati firewall.

Kelebihan dari jenis firewall ini adalah :

* 1. Lebih aman dibandingkan jenis firewall filtering router.
  2. Lebih mudah untuk melakukan pemeriksaaan terhadap data yang masuk pada level aplikasi.

Kelemahan dari jenis firewall ini adalah :

1. Adanya pemrosesan tambahan karena memiliki dua buah sambungan koneksi atau pemakai/ user dengan gateway.
2. Adanya proses pemeriksaaan gateway, kamudian baru meneruskan semua arus dari dua buah arah tersebut.
3. Circuit Level Gateway

Merupakan jenis firewall yang bekerja pada session layer. Pada jenis firewall ini pengguna luar tidak dapat melihat alamat IP jaringan internal pada paket-paket yang ia terima, melaluikan IP dari firewall.

1. Statefull Multilayer Inspection Firewall

Jenis ini merupkan kombinasi dari 3 jenis firewall sebelumnya, yaitu kombinasi dari packet filtering router, circuit level gateway, dan application level gateway. Jenis ini bekerja pada tiga buah lapisan, yaitu lapisan aplikasi, transport, dan internet. Jenis firewall ini dipasang pada bagian gateway kemudian melakukan pemeriksaan setiap atribut koneksi yang terjadi untuk setiap client dari awal hingga akhir koneksi dan sangat praktis untuk melakukan perlindungan jaringan yang kuat.