**FIREWALL**

[firewall](https://personalfirewall.comodo.com/what-is-firewall.html) merupakan sebuah sistem keamanan jaringan komputer yang berfungsi melindungi komputer dari beragam jenis serangan dari komputer luar. Firewall memonitor dan mengontrol semua lalu lintas jaringan masuk dan keluar yang kamu lakukan berdasarkan aturan keamanan yang telah ditetapkan. Secara umum, firewall komputer adalah program perangkat lunak yang mencegah akses tidak sah ke atau dari jaringan pribadi.Jadi, firewall adalah alat yang dapat digunakan untuk meningkatkan keamanan komputer yang terhubung ke jaringan, seperti LAN atau Internet. Firewall juga merupakan bagian integral dari kerangka kerja keamanan komprehensif untuk jaringan yang kamu gunakan. Firewall mampu menjamin keamanan melalui aktvitasi kontrol granular atas jenis fungsi. Firewall juga akan melangsungkan proses sistem yang memiliki akses ke sumber daya jaringan.

Cara kerja dari firewall adalah menganalisa paket data yang masuk dan keluar di dalam jangkauan aman yang terlindungi oleh firewall tersebut. Paket data yang tidak lolos dari analisis akan ditolak aksesnya baik masuk ataupun keluar jaringan yang telah dilindungi.Penyaring pada firewall atau filternya akan bekerja dengan memeriksa sumber paket data yang masuk dengan beberapa ketentuan yang dibuat untuk mengontrol paket yang dapat masuk. Sistem ini juga melakukan blokir jaringan tertentu dan mencatat lalu lintas paket data yang mencurigakan.

Komponen firewall adalah :

1. Passing
2. Blocking
3. Translating
4. Shaping
5. Forwarding
6. Logging

Untuk melaksanakan fungsi di atas firewall selalu membaca beberapa parameter yang menjadi bagian rulenya, adapun parameter tersebut adalah:

1. Alamat (IP) asal
2. Alamat (IP) tujuan
3. Port asal (/etc/services)
4. Port tujuan (/etc/services)
5. Interface
6. Protocol (/etc/protocols)
7. Options

Pada OS FreeBSD, firewall (layer 3) dapat di bangun dengan IPFW (IP Firewall), IPF (IP Filter). IPFW adalah firewall yang merupakan bawaan dari FreeBSD, sedangkan IPF adalah asli bawaan NetBSD dan FP adalah bawaan dari OpenBSD. PF ada dalam karnel FreeBSD mulai FreeBSD 5.3 dan sesudahnya.

Ketika komputer memiliki perlindungan firewall, semua yang masuk dan keluar dari komputer akan dimonitor. Firewall memantau semua lalu lintas informasi untuk memungkinkan ‘data bagus’ masuk, dan memblokir ‘data buruk’ memasuki komputer. [Firewall menggunakan satu atau lebih dari tiga metode](https://computer.howstuffworks.com/firewall1.htm) di bawah ini untuk mengontrol lalu lintas yang mengalir masuk dan keluar dari jaringan:

Penyaringan paket. Paket (potongan kecil data) dianalisis terhadap satu set filter. Paket yang lolos melalui filter dikirim ke sistem yang diminta, sementara paket lainnya dibuang. Layanan proxy. Informasi dari Internet diambil oleh firewall dan kemudian dikirim ke sistem yang diminta dan sebaliknya. Inspeksi stateful. Metode lebih baru yang tidak memeriksa konten setiap paket tetapi membandingkan bagian-bagian kunci tertentu dari paket dengan database informasi tepercaya. Informasi dari dalam firewall ke luar dimonitor untuk menentukan karakteristik spesifik, kemudian informasi yang masuk dibandingkan dengan karakteristik ini. Jika perbandingan menghasilkan kecocokan yang masuk akal, informasi tersebut diizinkan masuk. Kalau tidak, dibuang.

Firewall melindungi komputer individu atau seluruh jaringan dan merupakan tindakan pengamanan yang mirip dengan dinding di sekitar kota. Firewall menjaga komputer atau jaringan dan hanya mengizinkan masuk melalui titik akses terbatas setelah kriteria tertentu dipenuhi. Setiap paket data yang menghadapi firewall harus disetujui sebelum masuk ke dalam. Firewall memadamkan data apa pun yang tidak memenuhi kebijakannya, sebagaimana ditentukan oleh administrator firewall. Pengaturan yang salah atau konflik perangkat lunak dapat menyebabkan firewall memblokir semua entri data, meniru masalah konektivitas jaringan.

Firewall stateful sering tampil pada kecepatan yang lebih lambat daripada kapasitas tautan antarmuka jaringan mereka. Ini menyebabkan masalah ketika host dengan antarmuka jaringan yang lebih cepat daripada prosesor internal firewall mencoba mengirim data melalui firewall (TCP burst biasanya terjadi pada atau mendekati kecepatan data maksimum dari antarmuka host pengirim). Karena firewall harus buffer lalu lintas yang dikirim oleh host transfer data hingga dapat memproses semua paket dalam ledakan, ukuran buffer input sangat penting. Sayangnya firewall sering memiliki buffer input kecil, karena mereka biasanya dirancang untuk skala ke sejumlah besar aliran kecepatan rendah, daripada beberapa aliran data kecepatan tinggi. Jika buffer input firewall terlalu kecil untuk menahan semburan dari host transfer data, packet loss akan terjadi - seringkali menyebabkan masalah kinerja yang parah.

**IPDS**

Sistem pendeteksi gangguan (IDS – Instrusion Detection System) dan sistem pencegah gangguan (IPS – Intrusion Prevention System) merupakan teknologi yang relatif masih baru dalam masalah keamanan jaringan. Teknologi ini terus dikembangkan untuk dapat tetap up-to-date dengan perkembangan ancaman/gangguan terhadap komputer. Diprediksi sebagian dari pengembangannya mungkin diarahkan pada yang disebut proaktif intelijen IPS, yang secara aktif menghentikan ancaman/gangguan komputer. Proaktif intelijen IPS diharapkan lambat laun akan menggantikan IDS pasif yang hanya memantau ancaman/gangguan. Namun alih-alih mengganti IDS dengan IPS, organisasi/institusi mulai menerapkan kedua teknologi itu dengan cara menggabungkannya untuk memperoleh sistem keamanan jaringan yang lebih baik. Bahkan untuk menekan ongkos pembelian kedua alat itu, beberapa vendor mulai mengintegrasikannya kedalam sebuah alat yang disebut IDPS (Intrusion Detection and Prevention System).

Ternyata IDS dan IPS menjadi lebih baik ketika kedua teknologi itu diintegrasikan dalam sebuah alat. Ia dapat berfungsi sebagai sebuah virtual device, IDS pada internal dan IPS pada network perimeter. Dengan cara ini IDPS dapat mendeteksi keanehan-keanehan pada jaringan, sekaligus menghentikan serangan.

IDPS adalah peralatan keamanan yang kompleks yang menggunakan berbagai jenis teknologi pendeteksi untuk menemukan program-program jahat yang masuk kedalam jaringan dan menghentikannya sebelum worm, trojan, virus atau program jahat lainnya dapat merusak sistem. Bila hanya memasang IDS, sistem pendeteksi gangguan saja, alat tersebut hanya akan memberikan alarm peringatan adanya keanehan/gangguan pada sistem, dan administrator jaringan yang harus menyelidiki code mencurigakan yang dimaksud dan memutuskan tindakan selanjutnya. Bila selain IDS dipasangi juga IPS, maka code jahat yang ditemukan tersebut akan langsung dihentikan secara otomatis. IDPS melakukan kedua hal tersebut dengan menghentikan koneksi jaringan/user yang menyerang sistem, memblok user account yang berbahaya, IP address atau atribut lain dari pengaksesan ilegal terhadap server atau aset lain dalam jaringan. Atau dapat pula dengan mematikan seluruh akses ke host, service, aplikasi atau aset-aset lain dalam jaringan.

Beberapa IDPS cukup baik dalam meningkatkan kemampuan pengamanannya melawan serangan berbahaya. (1) menghentikan serangan melalui re-configuring peralatan kontrol keamanan pada network, seperti router dan firewall, untuk memblok akses ilegal. (2) menghentikan serangan melalui pemasangan patch pada host untuk menutup vulnerabilities. (3) menghentikan serangan melalui penghapusan code jahat yang ditemukan seperti men-delete file attachment dalam e-mail.

IDPS akan memberitahukan administrator jaringan tentang segala sesuatu yang menyangkut pelanggaran peraturan keamanan atau serangan yang terdeteksi. Pemberitahuan tersebut dapat melalui e-mail, web page, pesan dalam monitor IDPS user, perangkap SNMP (Simple Network Management Protokol), pesan syslog, atau program yang dibuat oleh user dan script. Umumnya pemberitahuan berisi data-data penjelasan tentang hal-hal dasar yang terjadi. Informasi yang lebih spesifik dikumpulkan dalam reports. Jumlah pemberitahuan yang dikirim oleh sistem sangat tergantung seberapa kuat level yang dipasang. Semakin kuat level keamanan yang dipasang maka semakin banyak pemberitahuan yang dikirimkan. Ketelitian pemasangan level keamanan akan sedikit banyak membantu menurunkan jumlah pemberitahuan, dan hanya pemberitahuan tentang gangguan keamanan tertentu saja yang dikirimkan.

[Manajemen keamanan informasi](https://hadiwibowo.wordpress.com/2006/10/03/menejemen-keamanan-informasi/) yang baik adalah kunci terlaksananya peraturan/regulasi yang dibuat. Dan itu adalah salah satu alasan pentingnya penerapan IDPS, terutama di organisasi yang menjalankan regulasi dengan ketat seperti institusi keuangan atau perusahaan kesehatan. Dengan menerapkan IDPS, sebuah perusahaan dapat mempertahankan akuntabilitasnya, memberikan kejelasan hak akses kepada user dan memberikan dukungan infrastuktur yang tepat. Peralatan IDPS tidak hanya melindungi sistem dari penyusup yang bermaksud jahat, tetapi juga melindungi gangguan yang disebabkan oleh kesalahan operasional user atau dari pembalasan dendam karyawan yang frustasi. Dari pengalaman perusahaan-perusahaan dalam beberapa tahun belakangan ini, gangguan keamanan sistem yang disebabkan oleh orang dalam ternyata cukup signifikan.

IDPS dapat dikonfigurasi sebagai alat untuk mengidentifikasi pelanggaran kebijakan keamanan dengan menset-nya seperti sebuah firewall. Juga dapat diset untuk memantau pengunaan akses yang tidak tepat seperti mentransfer file secara ilegal. Setting pemantauan user ini perlu diumumkan kepada para users, agar para users mengetahui bahwa setiap penggunaan akses akan dipantau. Hal ini diharapkan meminimalisir keinginan/usaha penyalahgunaan hak akses. Selain itu IDPS juga dapat menolong administrator untuk memelihara dan mempertajam kebijakan keamanannya. Sebagai contoh, IDPS akan memberitahu administrator jika didalam jaringan terdapat duplikasi setting firewall atau menangkap trafik mencurigakan yang lolos dari firewall.

Intrusion Detection Systems (IDSs) mendeteksi potensi serangan dengan memantau aktivitas di komputer dan jaringan. Pemantauan ini dilakukan dengan mengumpulkan dan menganalisis data yang berkaitan dengan pengguna dan organisasi. Data dikumpulkan dari berbagai sumber - seperti file log sistem atau lalu lintas jaringan - dan mungkin berisi informasi pribadi. Oleh karena itu, analisis data oleh IDS dapat meningkatkan banyak masalah privasi. Baru-baru ini, membangun IDS yang mempertimbangkan masalah privasi dalam kriteria desain mereka selain tujuan desain klasik (seperti kinerja dan ketepatan IDS) telah menjadi prioritas. Artikel ini mengusulkan taksonomi masalah privasi dalam IDS yang kemudian digunakan untuk mengidentifikasi tantangan dan masalah baru di lapangan. Dalam taksonomi ini, kami mengklasifikasikan data IDS yang sensitif privasi sebagai input, data bawaan dan data yang dihasilkan. Prototipe penelitian kemudian disurvei dan dibandingkan dengan menggunakan taksonomi. Teknik privasi yang digunakan dalam sistem yang disurvei dibahas dan dibandingkan berdasarkan efeknya pada kinerja dan ketepatan IDS. Akhirnya, taksonomi dan survei digunakan untuk menunjukkan sejumlah bidang untuk penelitian di masa depan.