**1. Pengertian Protokol**

**Protokol** adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras (hardware), perangkat lunak (software) atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras. Protokol digunakan untuk menentukan jenis layanan yang akan dilakukan pada internet. Salah satunya yaitu **TCP/IP.**

Sumber: <http://yuliantisafitri.wordpress.com/protokol/>

**2. 2 Jenis Lapisan Firewall ?**

**Firewall**  adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas [jaringan](http://id.wikipedia.org/wiki/Jaringan_komputer) yang dianggap tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang ([gateway](http://id.wikipedia.org/wiki/Gateway)) antara [jaringan lokal](http://id.wikipedia.org/w/index.php?title=Jaringan_lokal&action=edit&redlink=1) dengan jaringan Internet. Tembok-api digunakan untuk membatasi atau [mengontrol akses](http://id.wikipedia.org/wiki/Access_control) terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah *firewall* menjadi istilah lazim yang merujuk pada sistem yang mengatur komunikasi antar dua macam jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan berbadan hukum di dalamnya, maka perlindungan terhadap perangkat digital perusahaan tersebut dari serangan para [peretas](http://id.wikipedia.org/wiki/Peretas), pemata-mata, ataupun pencuri [data](http://id.wikipedia.org/wiki/Data) lainnya, menjadi kenyataan.

2 Jenis Lapisan Pada Firewall

1. **Personal Firewall**: Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditambahkannya beberapa fitur pengaman tambahan semacam [perangkat proteksi terhadap virus](http://id.wikipedia.org/wiki/Antivirus), *anti-spyware*, *anti-spam*, dan lainnya. Bahkan beberapa produk firewall lainnya dilengkapi dengan fungsi [pendeteksian gangguan keamanan jaringan](http://id.wikipedia.org/wiki/Intrusion_Detection_System) (*Intrusion Detection System*). Contoh dari firewall jenis ini adalah [Microsoft](http://id.wikipedia.org/wiki/Microsoft_Corporation) [Windows Firewall](http://id.wikipedia.org/wiki/Windows_Firewall) (yang telah terintegrasi dalam sistem operasi [Windows XP Service Pack 2](http://id.wikipedia.org/wiki/Windows_XP), [Windows Vista](http://id.wikipedia.org/wiki/Windows_Vista) dan [Windows Server 2003 Service Pack 1](http://id.wikipedia.org/wiki/Windows_Server_2003)), [Symantec](http://id.wikipedia.org/w/index.php?title=Symantec_Corporation&action=edit&redlink=1) Norton Personal Firewall, [Kerio](http://id.wikipedia.org/w/index.php?title=Kerio&action=edit&redlink=1) Personal Firewall, dan lain-lain. Personal Firewall secara umum hanya memiliki dua fitur utama, yakni *Packet Filter Firewall* dan [Stateful Firewall](http://id.wikipedia.org/w/index.php?title=Stateful_Firewall&action=edit&redlink=1).
2. **Network Firewall**: Network Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah [perangkat terdedikasi](http://id.wikipedia.org/w/index.php?title=Appliance&action=edit&redlink=1) atau sebagai sebuah [perangkat lunak](http://id.wikipedia.org/wiki/Software) yang diinstalasikan dalam sebuah [server](http://id.wikipedia.org/wiki/Server). Contoh dari firewall ini adalah [Microsoft](http://id.wikipedia.org/wiki/Microsoft_Corporation) [Internet Security and Acceleration Server (ISA Server)](http://id.wikipedia.org/wiki/ISA_Server), [Cisco PIX](http://id.wikipedia.org/w/index.php?title=Cisco_PIX&action=edit&redlink=1), [Cisco ASA](http://id.wikipedia.org/w/index.php?title=Cisco_ASA&action=edit&redlink=1), [IPTables](http://id.wikipedia.org/w/index.php?title=IPTables&action=edit&redlink=1) dalam sistem operasi [GNU/Linux](http://id.wikipedia.org/wiki/Linux), [pf](http://id.wikipedia.org/w/index.php?title=Pf&action=edit&redlink=1) dalam keluarga sistem operasi [Unix](http://id.wikipedia.org/wiki/Unix) [BSD](http://id.wikipedia.org/wiki/BSD), serta SunScreen dari [Sun Microsystems, Inc.](http://id.wikipedia.org/wiki/Sun_Microsystems) yang dibundel dalam [sistem operasi](http://id.wikipedia.org/wiki/Sistem_operasi) [Solaris](http://id.wikipedia.org/wiki/Solaris). Network Firewall secara umum memiliki beberapa fitur utama, yakni apa yang dimiliki oleh personal firewall (packet filter firewall dan stateful firewall), *Circuit Level Gateway*, *Application Level Gateway*, dan juga *NAT Firewall*. Network Firewall umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi [routing](http://id.wikipedia.org/wiki/Routing) untuk menentukan paket mana yang diizinkan, dan mana paket yang akan ditolak.

**3. Pengertian Malware?**

Malware (berasal dari kata malicious dan software) adalah perangkat lunak yang di ciptakan untuk atau merusak sistem komputer atau jaringan komputer tanpa izin dari pemilik

**Tipe dan jenis malware**

2 tipe paling umum dari malware adalah virus dan worm, kedua tipe ini dapat menggandakan dirinya (replikasi) dan menyebarkan dirinya sendiri, bahkan bentuknya dapat berbeda. Untuk dapat diklasifikasikan sebagai sebuah virus atau worm, malware harus mempunyai kemampuan untuk menggandakan dirinya. Perbedaannya adalah worm lebih mandiri sedangkan virus sangat bergantung ke file atau program tempatnya berada (host file). Berikut pengartian jelas dan definisi tipe malware lainnya.

**Virus**

Sebuah virus adalah tipe malware yang dapat menggandakan dirinya dengan memasukkan copy dari dirinya menjadi bagian dari program lain. Dapat menyebar dari satu komputer ke komputer lain, meninggalkan jejaknya yang berbahaya. Penyebaran dari virus ini biasanya menggunakan jaringan, file sharing, e-mail atau usb.

Hampir semua virus dijalankan bersamaan dengan file executable, yang berarti virus tidak dapat aktif jika user tidak menjalankan atau membuka file atau program yang berbahaya tersebut.

**Worm**

Worm serupa dengan virus, dimana mereka menggandakan dirinya dan menyebabkan tipe kerusakan yang sama. Perbedaannya adalah jika dalam penyebarannya virus bergantung atas file atau program berbahaya tempatnya berada, worm tidak. Worm adalah sebuah software yang berdiri sendiri dan tidak bergantung ke program atau file lain.

Penyebaran worm adalah dengan mencari kelemahan dari sistem atau membuat sebuah rik agar user menjalankannya. Worm kemudian memasuki komputer melalui kelemahan dari sistem dan mengambila keuntungan dari transfer file atau informasi di sistem, sehingga memperbolehkannya untuk menyebar secara mandiri.

**Trojan**

Trojan adalah tipe lain dari malware yang namanya mengikuti nama kude kayu yunani pada saat mereka memasuki troy. Merupakan potongan software berbahaya yang terlihat legal atau tidak membahayakan, hal inilah yang menipu user untuk menjalankannya. Sesudah dijalankan, ia dapat menyebabkan beberapa serangan seperti, menyebabkan rasa jengkel (membuka window baru secara terus menerus) atau merusak komputer (menghapus file, mencuri data atau mengaktifkan malware lain).

Biasanya tujuan utama trojan adalah memberikan jalan ke user lain untuk mengakses sistem. Tidak seperti virus dan worm, trojan tidak dapat menggandakan dirinya, mereka hanya menyebar melalui interaksi user seperti e-mail atau file di internet.

**Bot**

Didapatkan dari kata "robot" yang dimana merupakan sebuah proses otomatis yang berinteraksi dengan layanan jaringan lain. Bot dapat digunakan untuk tujuan yang baik atau jahat. Jika digunakan untuk tujuan yang jahat, bot dapat bekerja seperti worm dimana ia menggandakan dirinya dan menginfeksi komputer, bedanya adalah ia menunggu perintah dari si pembuat bot dalam melakukan pekerjaannya. Seperti mendapatkan informasi finansial, serangan dos, spam dan sebagainya.

**Sumber :**<http://www.tahupedia.com/content/show/137/Pengertian-Malware-dan-Jenisnya>