

5 December 2007

By: Ionut Ilascu, Editor, Software Reviews



## [Comodo's Security Reaching New Levels](#)

### *Defense+ to the rescue against malicious events*

Whenever I see an extraordinary freeware application I take a minute to come to my senses and then start looking for the catch. There must be something I did not take into consideration. And when that freeware's job is to protect your computer one way or another I commence some really serious digging for the details that may decrease its value. Most of the times the app is restricted for commercial use and can be employed only in the confinement of your home. But things are different with COMODO Firewall Pro. Because it is a Pro version one would expect to pay some amount of money for its services. It turns out that despite the fact that it provides very good protection for your system COMODO Firewall Pro is absolutely free. As they say on their website in the description of the product, **"It's Free. No Catch. No Kidding. Free for Commercial Use!"**. This statement shattered all my suspicions and made me proceed to its testing. Installing the product is complicated only if you want to as it can be added to the suite of programs the easy way or the hard way (this one involves a bit more configuration, that's all). Right from the launch of the installer you are prompted to cease the activity of any third party personal firewall by un-installing it. After a few steps that take you through the license agreement, installation location, etc. comes the junction: take the Advanced Firewall with Defense+ road or install the Basic Firewall. The difference between the two is that the first option is for experienced users and depending on your configuration it will increase the number of alerts while Basic Firewall is designed for users not familiar with computers and comes without Defense+ feature, thus resulting in less pop-ups on your screen. Going the rough, bumpy road for experienced users presents you with the choice for alerts. As COMODO can recognize over 1,000,000 applications due to the **internal certified executable database** you can configure it not to alert you in the case of certified applications or choose to ask you in the case of each application. Sure the first choice comes with less hassle and if you trust COMODO you can go with it. Otherwise, pick the second alternative for defining the rules for each application yourself. COMODO will automatically block all incoming connections without showing any alert and in the case of P2P applications this may pose a problem. Fortunately you can tell COMODO that you are a user of P2P apps therefore you want to selectively deny or allow incoming connection requests. **Defense+** is up next for configuration. Default settings bring maximum protection power for both new applications installed on the computer as well as those from non-fix drives like CD/DVD, network drives, USB keys, etc. For more flexible configuration users can customize the settings by selecting between three types of protection (Basic, Average or Advanced). And this concludes all the before installation settings for COMODO Firewall Pro. Next follows the actual inclusion of the firewall in the list of installed applications which ends with a request for computer restart. COMODO Firewall Pro will automatically place itself in the startup list in order to load with Windows and for you to benefit from protection each time your computer is started. The interface is easy to use and all the options are neatly organized in four distinct sections: Summary, Firewall, Defense+ and Miscellaneous. In the right side of Summary window the application displays all traffic currently flowing to and from your computer and the percentage for each connected application. With Defense+ the program will need a bit of time to learn how each installed application works so that it will bother you as little as possible. **Firewall Security** shield can be set on a scale from one to five, ranging from Disabled to Training Mode (application traffic initiated by software on your computer is learnt), Train with Safe Mode (only traffic of unknown applications pops up an alert), Custom Policy Mode (unless the app contains rules for its connection to be trusted you will be advised) and Block All Mode (no traffic is allowed). Training with Safe Mode is

the less intrusive security level for the firewall as it applies security policies, outgoing traffic of safe applications is learnt and you will be alerted for the unknown apps traffic. Alerts are also configurable, users having the possibility of enabling alerts for **TCP, UDP and ICMP** requests. A scale of five levels varying from Very Low to Very High sets the alert frequency level and the user has the possibility of being alerted for each port, both TCP and UDP protocols as well as for incoming and outgoing requests or IP addresses depending on the fixed notch. In **Firewall** section, for each "chapter" of the menu you benefit from a brief description so it's really not that big a deal handling all the options. From this section you have access to events and alerts triggered by a possible attack on the system, to defining trusted applications you know that cannot harm you (automatic "Allow" rule), blacklisting software, setting global firewall rules, viewing all active connections, setting ports for HTTP and POP3/SMTP connections, as well as defining privileged ones, adding new network zones or blocking them. In advanced section of Firewall settings you get to set the rules for different applications running on your computer. You have the power to block or allow the connection via some protocol (TCP, UDP, IP or ICMP) and the direction. You can specify which IP should a specific application be allowed to connect to, define an IP range, zone, host name or MAC address, the number of ports to be used in the process and the destination port. To make your life easier COMODO Firewall Pro brings a set of **predefined policies** specially tailored for web browsers, email clients, FTP clients, (un)trusted applications and for outgoing connections only. Users can enlarge the list by creating predefined rules of their own starting from a default type of application. This way you can apply them automatically to other programs as well without having to go through the configuration task each time. The **flexibility** of this firewall is quite elevated allowing users to set the characteristics of an intrusion. That means the users can define TCP, UDP and ICMP flood parameters by setting traffic rate and duration values and the block time of a host complying the users-set requirements to qualify as intrusion. Defense+ comes to complete COMODO Firewall but the way I see it it'll just give you a headache at the beginning. During our testing it was always learning something new, even when I would simply move files from one partition to another. It cooled down at one point but as new actions were performed on the computer each time there would be an alert in the lower right corner of the screen telling me that Defense+ was learning. Despite the fact that it can be really annoying at times, Defense+ strengthens the protection of the computer by monitoring activities such as interprocess memory access, **windows/WinEvent hooks**, device driver installation, **loopback networking**, process termination, window messages, DNS client service. It can also monitor against modifications COM interfaces, registry keys, protected files and folders and monitor direct access to physical memory settings, computer monitor, disks and keyboard. This way in case some nasty tries anything behind your back Defense+ will be there to alert you of any attempt and you get to block or allow the activity. Nevertheless, it proves to be a nag when installing/un-installing applications as it prompts for your opinion almost on every action. It comes in handy though when you decide to install a new application on your computer and once it has learned the details of the activity it'll leave you alone. COMODO Firewall Pro in particular and COMODO in general has come a long way. During our testing, with adequate settings it managed to pass quite stubborn firewall leak tests (PCFlank is one of them) not allowing surreptitious transmission of data to a remote location. However, in some tests it failed to properly seal some ports and it only closed them but did not stealth them. Even so, it makes for a great protection of a PC and not only. It is not too difficult to configure and an average user should not have any problems with setting it up, especially when it explains the purpose of each option it incorporates. Defense+ feature available in Comodo Firewall Pro will monitor the activities of all executables and warn you each time an unknown file is trying to run. Activating it gives the user the chance to select which executable is allowed to run on the PC and which is not. However, this can get a bit frustrating and nagging at times especially if you are used to installing all sorts of applications on the computer on a frequent basis. But it can be

permanently deactivated and the cost is a system restart (sure, dealing with all the threats falls on your shoulders). **The Good** Installs in a jiffy and it takes little time and effort to complete its configuration. You benefit from snippets of information on each major feature of the application so you will not be left in the dark. The firewall is one of the best on the market and properly configured it offers one of the tightest means of protection for your computer. Users have maximum flexibility with regards to setting up the policies for handling the connections. Active Connections view summarizes at a glance currently active connections for each application providing information on the amount of incoming/outgoing data, source IP and protocol used for the entire activity. Defense+, though a nag at some moments, monitors all activity going on on your computer alerting the user in case some mischievous nasty tries to pull something behind your back. **The Bad** Defense+ tends to be a little too defensive at some points and takes a while to learn all the going ons on a system. On the other hand, it alerts the user in case of an abuse and provides the means of blocking the activity of malware on the system. **The Truth** Comodo Firewall Pro is a hell of a protecting tool, actually one of the best currently on the market as it comes with a very user friendly interface, easy to understand options and plenty of flexibility with regards to both firewall and Defense+ feature. Defense+ can be permanently deactivated and the firewall will keep on protecting the system unhindered. During our testing it prevented leakage of information to remote locations but in some tests it failed to stealth up the ports, although all of them were closed. All in all Comodo Firewall Pro does a stupendous job with deflecting surreptitious attacks and the fact that it is an absolute freeware (it can be used commercially as well) only adds more value and turns it into a general preference of the users. *Here are some snapshots of the application in action:*