

## Re: Sygate Free PFW

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-06/msg00403.html>

---

- *From:* "WinTerMiNator" <[me@xxxxxxxxxxxxx](mailto:me@xxxxxxxxxxxxx)>
  - *Date:* Sun, 11 Jun 2006 21:18:48 +0200
- 

Volker Birk wrote:

Shadowman <[shadowman@xxxxxxx](mailto:shadowman@xxxxxxx)> wrote:

I've been using the free Sygate PFW in combination w/ a Linksys router/switch

...

However, since the product is no longer updated, I wonder if it is still a valid solution since any recently discovered flaws or security holes won't be fixed. Opinions? Is it a good idea to just switch to the windows XP SP2 firewall?

Yes.

No. Keep Sygate PFW. Version 5.5 build 2710 preferrably (latest one has been modified in order Windows useless security center be aware of Sygate; but it doesn't have any security improvement and this latest and last version is very buggy!).

First, Windows firewall does not inform user when an apps tries to connect to internet: it knows to block only inbound connexions, not outbound ones.

Volker and his fellows will say you it is a good design choice! Even if this was true, Windows firewall has definitely a big hole: when apps are installing, they can add an exception and so allow an *\*inbound\** connexion without requesting user's authorization or even without informing him (her). For example, just try to install Skype 2.0, or any security product which needs to connect to internet...

This arrives, of course, when app is installed in a session where user has admin rights (note that almost all windows apps require an admin session to be installed); it arrives also when app is installed invoking "runas", or when app is launched using "Psexec" (an utility from Mark Russinovitch) which gives the app the execution rights of "SYSTEM" user.

Of course, what legitimate apps can do, malware can also do. And several malware can install themselves using Psexec or similar method and can have

## Re: Sygate Free PFW

so full access to add exceptions.

—> Windows firewall is not a firewall, it is like a sieve!

Better in this case to have a firewall that requests user's authorization when an app tries to connect to internet...

Note that no software firewall can give you an absolute security:

– A firewall is normally done to prevent unwanted packets to reach the target machine; and a software PFW runs on the target machine! Big contradiction... packets have reached target machine when they are intercepted by PFW.

– PFW can have their execution stopped.

– They can be deceived by malwares attempting to connect.

However, among PFW's, Sygate PFW is probably, not the best, but the "least bad". It has an unique possibility to distinguish when an application which wants to connect is launched directly by user or launched by another app; in the second case it will request user's authorization (here is one Volker's proofs of concept defeated...).

It also seems to be less targeted by malwares than Windows firewall.

My recommendation:

– If you can afford it, buy a NAT / firewall / modem-router; for example US Robotics 96107.

– And use Sygate PFW complementary, to add fine tuned advanced rules (filter hosts, protocols) and filter your outbound connexions (too many softwares want to "phone home" without your authorization).

But don't bet your life on the fact Sygate PFW will detect and block all malwares wanting to connect! It should be used in a secure environment (windows with full security patches applied; a good antivirus software; web browsing with high security level, javascript / java / Active X disabled; antispysware; and, if you are paranoid, intrusion detection software...). And even in that case you cannot be sure your computer will not be damaged by a malware.

In fact, a computer should not, for security reasons, be connected to internet! ;–)

So, never forget to periodically backup your computer! You might need, one day, to recover from a crash, induced by malwares or whatever else.

Yours,  
VB.

Regards

—

Re: Sygate Free PFW

Re: Sygate Free PFW

Michel Nallino aka WinTerMiNator

<http://www.winterminator.co.nr> (Internet et sécurité)

<http://www.gnupgwin.co.nr> (GnuPG pour Windows)

Adresse e-mail invalide; pour me contacter:

<http://www.cerbermail.com/?vdU5HHs5WG>