



*internet business success*

## How To Set Up A Firewall

*...real protection - right now - for free*

**By Sam Stephens, 2004**  
**TacticalSuccess.com**

### **FREE Distribution:**

Feel free to distribute this information to anyone you may think can use it, as long as:

- You do not sell, rent or in anyway accept money for this information – this information is meant to help people, and taking money for that is just not a nice thing to do.
- You do not modify this information. I've made this document as accurate as possible, therefore does not require modification.

### **Copyright:**

Written by Sam Stephens, April 2004. All writing and graphics held within this document are copyrighted material, and in being so cannot be used, modified or distributed without the authors express consent.

The views held within this document are strictly the personal views and experiences of the author, and in no way do we guarantee the outcome of the reader's business activities. While the information contained within is as accurate and specific as possible, TacticalSuccess and Sam Stephens cannot control or be held responsible for the way this information is used or implemented.

## **Firewall. It's like putting a front door on your house.**

Most people leave their computers unprotected. Installing a firewall is like putting a front door on your house. Without it people can just waltz on in and steal food from your refrigerator.

It really is a common and real security issue that can easily be remedied...for free!

## **SO WHAT IS A FIREWALL?**

A firewall is a security wall to separate your computer from the Internet. These actually come in a few different forms:

- Hardware – large companies actually use a whole computer as a firewall
- Peripherals – you can even buy firewall boxes that plug in to your network connection that acts as a firewall
- Software – firewall software can be installed on your computer to stop people from breaking in to your computer

We're going to install a firewall, and in doing so we're aiming to stop:

- Hackers
- Script Kiddies
- Viruses
- Trojans
- Privacy Breakers

### **Hackers**

Hackers, well we've all heard of hackers – the reality of it is that some hackers are good and some hackers are bad. All hackers like to break security, to test the limits of machines and to see if they can outsmart or find a soft-spot in a website/computer/server/software security system. It's what they do after they've broken in that defines a good or a bad hacker. Personally I'd like to keep all of them out.

### **Script Kiddies**

Script kiddies are kind of like hackers, but instead of doing the hard work themselves, they rely on software applications or scripts that test security soft-spots for them. All they do is open the software and click "go". They can be very dangerous – why? Because there is potential to be a lot of them around, and the tools that they use are usually written by a very smart hacker.

### **Viruses**

Not long ago there was a virus that went around the web and it would keep resetting your computer as soon as you logged on to a live internet connection. The reason it reset your computer was NOT because that's what it was made to do, it was because of a side-effect. The virus was designed to automatically send itself to IP addresses and spread directly to people's computers.

Note: An IP address is basically a number that identifies your computer on the network – in this case the network is the internet.

Interestingly enough there was a secondary virus that spread itself in the same way who's job it was to seek out and destroy the original virus. It almost sounds like something out of Terminator.

## Trojans

Trojans are basically in the same camp as viruses. Trojans however, are software applications that have a hidden secondary purpose. A lot of them open up “backdoors” to your computer so that people can log on to your computer over the internet and take control of it.

## Privacy Breakers

Some software try's to connect to the internet with no apparent reason. I've seen software that has no reason to connect to the net, try and connect. As far as I'm concerned, unless the software has a very good reason to log on to it's designer's server, I'm not letting it.

## SCRIPT KIDDIES GET OUT OF MY PLAYGROUND!

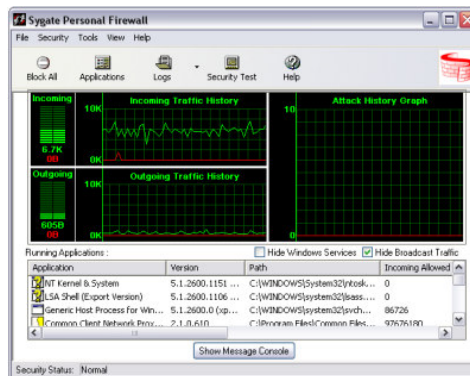
A firewall is the only way to keep things out, and in the case of privacy breaker's, information in.

Firstly we need to decide what kind of firewall we want. For home and small office use, a software-based firewall is fine.

You can purchase different firewalls however one of the best firewalls I've found is free for personal use.

Sygate Personal Firewall.

This is the one that I use, and the one I recommend other people use, and also the one I'm going to show you how to install today.



(Sygate's main screen)

Firstly, we need to download Sygate.

[www.sygate.com](http://www.sygate.com)

Check out the products link, and find the link to download the free Sygate personal firewall. They do also sell software applications on this website, so make sure you choose the free version!

Once the download is complete, find the file you downloaded, and double-click it.

This will run through the Sygate installation, which is pretty straightforward. It's just a standard install package, and it won't ask you any tricky questions.

After installation is complete you'll need to reboot your PC before it's ready to go.

## **LIVING WITH THE NEW FIREWALL IN MY LIFE:**

Once we've rebooted you'll notice a new icon in your system tray. It's two arrows, one pointing up, one pointing down. This means Sygate is now running, and your computer is protected.

The fantastic thing about Sygate is that it just runs in the background and you don't really need to touch it.

### **Keeping Things In:**

Configuring Sygate is performed as you go about your day-to-day internet work. When you start up a new application that Sygate hasn't seen before, it'll pop up a box saying "Do you want to allow this program to access the network?"

If you trust the application, click Yes. If you always want to allow it to connect, then tick the "Remember my answer" tick-box. From now on, whenever this application tries to connect to the internet, your firewall will allow it to.

I'd recommend allowing your internet browser, your email software and any other software that uses the internet to always allow connection.

Software that you're not sure about, or only occasionally want to allow to access the internet, you can decide on a case-by-case basis.

Software you never want to connect to the internet, such as those applications that you don't think should be, click No and remember my answer.

You may even find software connecting to the internet that you didn't even know tries to!

### **Keeping Things Out:**

Sygate automatically stops attacks and port scans. You don't even have to lift a finger.

Sometimes you may be asked if you'd like to allow someone or something to connect to your machine. Unless you know who it is and why they're connecting to your machine, click No.

And it's as simple as that. You've got firewall protection!

Wishing you all the success you could possibly handle,

**Sam Stephens**



*Director*

**TacticalSuccess Enterprises**

<http://www.tacticalsuccess.com>

*"internet business success is easy when you know how"*

## **SUMMARY:**

Now that you have your firewall installed, you're protected from most attacks. Keep in mind that a firewall does not protect you from most viruses, and as with any security tool you should also use caution when interacting on the internet. The firewall is there to help, but it's not a replacement for carefulness.

To keep your computer clean, it's also a great idea to scan your computer for virus's, set up a firewall and also scan for adware/spyware often.

More ebooks relating to these procedures will be available at:

<http://www.tacticalsuccess.com/tech>

## **WHO AM I:**

This ebook was written by myself, Sam Stephens, CEO of [TacticalSuccess.com](http://www.tacticalsuccess.com).

TacticalSuccess.com offers real-world solutions to internet business. I've stood in boardrooms full of directors and high-level management for private and government organisations, and I've convinced them to purchase \$80,000 products and systems. I was taught sales techniques from some of the best sales managers in the business, and was relentlessly drilled each week until I perfected my presentation skills.

This experience not only made me a very comfortable living while I worked for the company, but it also gave me the experience and insight to bring these skills into the internet business world – a world I've now had over 7 years experience in.

**Remember: *Internet Business Success Is Easy When You Know How!***

<http://www.tacticalsuccess.com/>