

## Re: Personal Firewalls

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-04/0160.html>

---

**From:** e2chameleon ([e2chameleon@btopenworld.com](mailto:e2chameleon@btopenworld.com))

**Date:** 04/10/03

Date: Thu, 10 Apr 2003 00:12:40 +0100 (GMT Daylight Time)

From: "e2chameleon" <[e2chameleon@btopenworld.com](mailto:e2chameleon@btopenworld.com)>

To: <[sridhar.javaraman@wipro.com](mailto:sridhar.javaraman@wipro.com)>, <[security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)>

Hi,

There are tools available that perform additional analysis of logs in ZoneAlarm and Black Ice PC Protector. VisualZone Report Utility is a free add-on for ZoneAlarm and ZoneAlarm Pro that enhances the reporting and tracing abilities of the products (including intruder tracing via maps). It can do real-time reporting of alerts and also includes functionality to automatically report abuse to ISP's and to the DShield.org web site. Further information, including the download, can be found at <http://www.visualizesoftware.com>. ZoneLog Analyser is a cheap add on for ZoneAlarm and ZoneAlarm Pro that provides on-demand analysis of the logs. It can also be used to report abuse to ISP's and send information to Dshield.org. You can filter reports and produce graphical analysis. Go to <http://www.zonelog.co.uk> for further details, including the evaluation and registered downloads. The Visualice program from zonelog provides similar functions for BlackIce PC Protector.

The ICSA Labs test and certify security related products as does West Coast Labs. They provide an independent view on the abilities of products to perform to high standards. Their web sites are at <http://www.icsalabs.com/index.shtml> and <http://www.check-mark.com>. Check out the Gibson Research Corporation's Shields Up site at <http://grc.com/su-firewalls.htm> for information on how personal firewalls work and the Home PC Firewall Guide provides independent reviews of Internet security products including personal firewalls. The site is at <http://www.firewallguide.com/>.

I did some research last year on personal firewalls and found a few, listed below.

### Agnitum Outpost Firewall

This product, developed in the open source environment is the first personal firewall to be able to use plug-ins so that third party developers can write enhancements for it. There are 2 versions, Free and Pro. The free version includes intrusion detection, can disable advertisements, stop access to

## SecurityFocus BASICS: Re: Personal Firewalls

objectionable site either by site name or keyword and block active content (such as Java and ActiveX). It can also block malicious code in incoming files and supports 3rd party virus checkers. It can "stealth" the ports on your computer making it appear invisible to potential intruders. See <http://www.agnitum.com> for further information, including the download.

### BlackICE PC Protection

(Formerly BlackICE Defender) monitors incoming and outgoing communications and alerts when suspicious activity is detected. It protects against malicious activity in both applications and Internet protocols. Alerts are colour coded depending on severity and there are 4 levels of protection depending on the level required. It is updated regularly keeping users protected against the latest threats. More information can be found at <http://www.iss.net>.

### Checkit Firewall

Blocks unauthorised incoming and outgoing communications (applications and protocols). The product also includes vulnerability analysis capabilities to identify possible weaknesses in your configuration. For more information go to <http://www.smithmicro.com>.

### eTrust EZ Firewall

Prompts you to you allow or deny local applications or services access to the Internet as well as remote connection requests to your PC. The results are remembered for the next time. There are pre-set rules and you can fully customise them for your own needs as well as download configuration updates from the web. Online reports and analysis of attacks are available. Can be purchased on its own or as part of the EZ Armor suite. More information, including a trial download, can be found at <http://www.my-etrust.com>.

### Freedom Personal Firewall

Stops intrusion attempts and allows you to decide which of you applications is allowed to access the Internet. You are alerted when suspicious activity is detected and all incidents are logged. Advanced configuration and personalisation is available but you don't need to be an expert to be protected. In addition to firewall functions the products also comes with password encryption and management, advert blocking, personal information protection, cookie management and automated form filling. For more information, and to purchase the product, go to <http://www.freedom.net>. The product is also available are part of the Freedom Privacy and Security suite

### Kerio Personal Firewall

This product allows you to choose between three different levels of security You can block only specified items, get the application to prompt you when new items on your computer try and access the internet or try and access your computer from the Internet. You can also block all network activity. The rules can be customised to your personal requirements. Your computer is hidden from potential attackers using stealth technology and it can be administred over the Internet using a secured connection. The product is free for home / personal use and can be found at <http://www.kerio.com>.

### Look 'n' Stop Lite

This uses Internet filtering to make your computer invisible to potential attackers. Logs can be analysed. See <http://www.looknstop.com> for further details, including the free download. Another version that includes application filtering is available to buy.

### McAfee.com Personal Firewall

The service monitors Internet activity and defends your PC from hackers and Internet attacks. You are alerted to suspicious activity as it happens and provides you with detailed information of the events. It has links to Hackerwatch.org, an online anti-hacker community where you can and get information on the best method of response to an intrusion attempt and report your incidents to online authorities. A "Plus" version of this subscription service includes the ability to trace intruders and in depth information on the events. The products also integrate with McAfee's free SecurityCenter which lets you check how secure your PC is and view the latest security and virus alerts. More information can be found at <http://www.mcafee.com> or <http://uk.mcafee.com>.

### Norman Personal Firewall

Analyses each application that attempts to connect to the Internet or your local network from your computer. Incoming connections and scripts are also monitored. Your visibility on the local network and access to your local shared can also be configured through the personal firewall. You can set which Internet sites are allowed to run active code on your equipment. Access to web sites can be controlled based on the address or words used in the site and different users can be granted access to different sites. Time allowances can also be assigned to users to control browsing time. Cookie and web advert management is also included. Executable files are checked to ensure that malicious code is not masquerading as a real file to cause damage. For more information go to <http://www.norman.com>.

### Norton Personal Firewall

Automated configuration sets up rules for most Internet based applications. Controls and incoming and outgoing traffic. Alerts you to suspicious activity. Prevents personal information from being sent to unprotected sites without your knowledge. Blocks systems trying to probe your computer for weaknesses. The system can automatically confirm what applications can safely access the Internet and which can't. Can detect equipment on your home network which can be safely added to your trusted zone. Easy configuration. One year of Intrusion Protection updates included in the licence. More information can be found at <http://www.symantec.com>. The product can also be purchased as part of Norton Internet Security 2003 (which works out cheaper in the long run).

### Pathlock e100 NETimer

This isn't a firewall but a hardware option to physically disconnect your PC from the Internet when you aren't using it. It's ideal for broadband "always-on" connections as it reduces your visibility to potential attackers when you are not actively using the Internet. It also contains a timer to

## SecurityFocus BASICS: Re: Personal Firewalls

disconnect you after an hour. For more information go to <http://www.pathlock.com> or <http://www.pathlock.dk/> for European sales.

### PC-Viper

Allows you to allow or block various protocols (Internet communication file types). You can also decide what applications you want to allow access to the Internet and alerts you when any suspicious activity takes place. It can also make your PC appear invisible to hackers to increase protection. There are 3 levels of content security to stop pornographic material from being viewed. This product records all traffic (in and out) and can provide statistics. Configuration can be password protected to dissuade tampering. More information, including trial download and product purchase/registration can be found at <http://www.pcviper.com>.

### Preventon Personal Firewall

This product protects against hacking attempts and Trojan Horse attacks. Alerts and colour coded logs let you understand what has taken place. The interface has been designed to allow you to work securely without being an expert. More information can be found at <http://www.preventon.com>.

### PrivateFirewall

This product continuously monitors your system and can automatically modify certain settings that could allow unauthorised access. Sensitive system areas are monitored and you are given reports to help you decide on any configuration changes that may be required. When first installed it evaluates your system and automatically modifies certain system settings to ensure security. Further information can be found at <http://www.privacyware.com>.

### Sygate Personal Firewall

Prompts you to allow or deny local applications or services access to the Internet as well as remote connection requests to your PC. The results are remembered for the next time. Allows you to trace the attacker so that you can make a complaint to the system owner or ISP. Email notification can be set up to notify someone whenever an attack is taking place. Attack and Traffic history graphs are available and various log files are generated so you can check what's been happening on your system. Attacks are rated on different levels of severity. A Pro version includes updateable attack signatures and more configuration options. More information, and the download, can be found at <http://www.sygate.com>.

### Tiny Personal Firewall

Prompts you to allow or deny local applications or services access to the Internet as well as remote connection requests to your PC. The results are remembered for the next time. Log files, detailing events can be sent to a central server. There is also a corporate version of this called Centrally Managed Desktop Security. Can be configured remotely and time dependent rules can be set up to only be valid at certain times (to only allow online gaming at a certain time of day for instance). More information and the download, can be found at <http://www.tinysoftware.com>.

## SecurityFocus BASICS: Re: Personal Firewalls

### VisNetic Firewall

Starts protecting your system as soon as you boot up and can be configured for multiple network adapters. Real-time activity viewer lets you see what is happening at any time. Time based rules allow you to allow access to resources at only certain times. Comprehensive logging is available and the file can automatically be emailed to an administrator and can alert when a rule is triggered. Further information including trial download and product purchase can be found at <http://www.ccssoftware.ca>.

### ZoneAlarm

Prompts you to allow or deny local applications or services access to the Internet as well as remote connection requests to your PC. The results are remembered for the next time. Limited email protection is also included. The product can "stealth" the ports on your computer making it appear invisible to potential intruders. Another version (ZoneAlarm Pro) with additional functionality is also available. Alerts are colour coded based on severity and incident analysis is available online.

-----Original Message-----

From: Sridhar J  
Date: 09 April 2003 00:48:49  
To: [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)  
Subject: Personal Firewalls

Hi

I have a PIII 550 m/c running Win98. I need a personal firewall for it. I am looking at Zone Alarm, Sygate and Tiny Personal Firewall as my options.

My intention is not only to protect my systems, but also to learn something about logs and analysing them. In light of this, which do you think would be ideal?

No, I don't have a \*nix system and don't intend to use it now.

-----  
Regards  
Sridhar J  
-----

"What you do in this world is a matter of no consequence;The question is, what can you make people believe that you have done."  
—Sherlock Holmes in "A Study in Scarlet"

-----  
Is SPAM over-loading your e-mail server, disk space or bandwidth?  
SurfControl E-Mail Filter is flexible, intelligent and policy-driven protection.

Re: Personal Firewalls

SecurityFocus BASICS: Re: Personal Firewalls

<http://www.securityfocus.com/SurfControl-security-basics2>

Download your free fully functional trial, complete with 30-days of free technical support.  
Stop SPAM before it stops you.

---