

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Windows Firewall vs. ZoneAlarm: A Comparative Analysis

Russell W. Robinson
GCWN Practical, Ver. 5, Option 1
October 15, 2004

ABSTRACT

The principal aim of this paper is to provide a solid starting point for anyone looking to accurately gauge the overall effectiveness of Windows Firewall, a key component of Windows XP Service Pack 2. Currently the average person knows relatively little about the various configuration and deployment options, potential pitfalls, and comparative strength of Windows Firewall, but Microsoft's aggressive new strategy in the arena of patch management will inevitably force many to learn by trial and error. Armed with a thorough understanding of how to implement and work with Windows Firewall, however, along with an awareness of its limitations, everyone from the average home user to the seasoned system administrator will be able to incorporate it into an effective defense-in-depth strategy.

This paper will see Windows Firewall pitted up against ZoneAlarm in an apples-to-apples comparison, and should clearly demonstrate the strengths and weaknesses of each. During the course of this paper the reader will learn that, while Windows Firewall is certainly a big step in the right direction for Windows security, it is not, and was never intended to be as feature-rich or robust as ZoneAlarm, or the vast majority of 3rd party personal firewalls available today. In addition, those looking for an answer to the question "If I already have Windows Firewall enabled, do I *still* need a third-party firewall such as ZoneAlarm?" will discover that they do in fact need some of the additional benefits offered by a product such as ZoneAlarm, in order to achieve a reasonable level of security.

SECTION 1

One of the most significant changes brought on by Service Pack 2 for Windows XP (released September 2004) is the new and improved Windows Firewall, which has been completely redesigned and hardened, with its "on by default" setting generating much applause within the global security community. However, many are still a bit hesitant to download and install Windows XP Service Pack 2, even though it has been available for nearly two months at the time of this writing. The aversion for some may be rooted in poor experiences with prior Windows service packs (Windows XP Service Pack 1 immediately comes to mind), while others are tech-savvy enough to realize that a properly

© SANS Institute 2004 Author retains full rights.

updated antivirus application, coupled with a fully-patched Windows installation and a properly configured third-party firewall provide just as much (or more, most would argue) protection against various security threats. Incidentally, many of those same tech-savvy users are subscribers to the notion that Microsoft has been more concerned with bolstering their position atop the software world than they have been with security, as if Microsoft were saying "we want you to believe we've always been thinking of security, when we've really been thinking about marketing and the next product cycles."[1] Microsoft's true motives and initiatives notwithstanding, the introduction of XPSP2 marked a dramatic shift in Microsoft's efforts to secure the Windows desktop.

The new Windows Firewall replaces the much-maligned and relatively ineffective Internet Connection Firewall (ICF) which shipped with the first build of Windows XP. ICF was *disabled* by default, and required users to dig fairly deeply into the OS to enable and/or configure it (a user needed to go to a connection's Properties, then the Advanced tab, and lastly check a single box with the caption "Protect my computer and network by limiting or preventing access to this computer from the Internet"). An IPV6 version of ICF was later released by Microsoft as part of the Advanced Networking Pack for Windows XP, but it too was scarcely used due to its low profile in the GUI. In addition, both versions had a tendency to break File and Print sharing.

Many Windows users who successfully enabled and configured ICF, and who stayed on top of developments in the world of information security soon discovered that ICF had some pretty serious weaknesses, such as:

1) It lacked the ability to separately configure firewall settings for each network interface installed on the computer- there was only one universal configuration for all interfaces

2) It did not offer egress filtering (monitoring of outbound connections)

3) It provided no visual alerts regarding blocked access attempts or dropped packets, and no reporting capability (other than log files)

4) It left the OS in a vulnerable state for a brief period during bootup.[2]

Windows Firewall, on the other hand, was specifically designed with some of these issues in mind, and Microsoft is now touting it as a much more secure solution.

According to Microsoft spokesperson Greg Sullivan, "only 10 per cent of Windows users have a personal firewall on their systems."[3] With internet worms, Trojans, and other malicious software now reaching pandemic proportions, it is

[1] http://searchwin2000.techtarget.com/originalContent/0,289142,sid1_gci860936,00.html
[2] http://www.consumersearch.com/www/computers/firewalls_internet_security_software/
[3] http://news.zdnet.com/2100-1009_22-5301625.html

© SANS Institute 2004 Author retains full rights.

difficult to understand the mindset of internet users who continue to operate their computers without sufficient protection. Perhaps they feel that it's simply inconvenient to be bothered with learning new software. Perhaps many of those who have tried personal firewall solutions such as ZoneAlarm quickly grew weary of all the prompts for program access and simply said "enough is enough". Still others, despite all the industry buzz and media attention surrounding malware and internet security, may not even have a clue what a firewall is, what it does, and why they even need one.

Firewalls are an integral part of just about any effective defense-in-depth strategy, and the need for them transcends any perceived boundaries between operating systems and their respective susceptibilities to attack. All un-firewalled versions of Windows are certainly at risk, but for the purposes of this paper we will focus exclusively on Windows XP with Service Pack 2. Like countless Windows users have already discovered, and undoubtedly many more will in time, choosing to operate an internet-facing computer without a firewall can be likened to playing Russian roulette- eventually you *will* get nailed.

Although hundreds of millions of Windows XP users worldwide will have downloaded and installed XPSP2 by the time Longhorn comes to fruition, it will be interesting to see how much more secure their computers really are in the interim. Those aforementioned folks who are only vaguely familiar with firewalls might think that XPSP2 has suddenly made their computers completely impervious to attack, and almost any security practitioner would argue that such a false sense of security is more dangerous than no security at all (people are much more willing to engage in riskier behaviors under the auspice of protection and immunity than they would otherwise). Even with XPSP2 and thus Windows Firewall installed, computer owners who fail to *actively* manage security on their computers, while at the same time employing a defense-in-depth strategy, will eventually fall victim to attack. Simply put, Windows Firewall by itself is not bulletproof, nor is any 3rd party personal firewall.

So the question then becomes, "among the available options, which firewall is the best one for the job"? Most would generally agree that the optimal solution to this problem is a firewall application that is 1) easy to obtain and install, 2) comes pre-hardened and pre-configured with an effective rule set offering maximum security, and 3) is very low-maintenance. In this paper we will examine Windows Firewall and ZoneAlarm side by side, and try to determine which of these (if either) satisfies these requirements, and to what degree. In other words, we'll let the numbers and facts do the talking.

SECTION 2

I felt compelled to write about Windows Firewall primarily because XPSP2 is still a relatively hot topic in information security, yet I'm finding more and more that people really aren't very knowledgeable about it, save for a vague familiarity with some of the key buzzwords. In addition, as a security administrator in a healthcare organization I have been tasked with researching XPSP2 and developing a plan for rollout at 4 regional hospitals. The function and behavior of

© SANS Institute 2004 Author retains full rights.

Windows Firewall is of particular concern, since hospitals are known for harboring a myriad diverse and specialized applications, and unplanned system failures and downtime can have devastating consequences in terms of patient care.

For the purposes of comparison, I chose ZoneAlarm from Zone Labs (http://www.zonelabs.com) simply because it seems to be the most popular of the third-party firewalls available today, and it would likely be the solution most people would turn to as an alternative to Windows Firewall. I drew this conclusion partly from personal experience and partly from the fact that the most popular firewall being downloaded from the Security & Encryption section of the Download.com website is ZoneAlarm, with around 33 million downloads at the time of this writing. The closest competitor is Sygate Personal Firewall, with a comparatively paltry 2.7 million downloads.

So now that we've identified the reasons why each firewall solution was chosen, let's move on to the detailed analysis and testing.

Windows Firewall

Windows Firewall (abbreviated WF from this point forward) can only be installed as a component of Windows XP Service Pack 2—you will not find it available as a stand-alone app. Microsoft has provided a number of avenues through which XPSP2 can be acquired, including the methods listed below[4]:

- Automated download via the Windows Automatic Updates Client (assuming the AUC has been configured to do this- if not, Microsoft has provided a link which will automatically enable the AUC: http://www.microsoft.com/athome/security/protect/windowsxp/choose.aspx)

- Download and install on-demand via Microsoft's Windows Update website: http://windowsupdate.microsoft.com

- Direct download of the entire service pack in a single executable: http://www.microsoft.com/athome/security/protect/default.aspx

- A free Compact Disc, with ordering available at the following URL: http://www.microsoft.com/athome/security/protect/cd/confirm.aspx

WF is referred to as a "stateful host-based firewall". For those unfamiliar with this term, here is a brief explanation of its meaning: "stateful" indicates that it maintains a list (or table, more specifically) of all requests made for internet access by locally installed applications and/or services. Inbound data packets from the internet are examined and cross-referenced against this table, and any

[4] Installation and troubleshooting information can be found in the Windows XP SP2 Support Center at: http://support.microsoft.com/default.aspx?scid=fh;EN-US;windowsxpsp2

© SANS Institute 2004 Author retains full rights.

unsolicited data which was not specifically requested by an application/service in the table is discarded and ignored (unless an exception has been defined in the firewall's configuration- more on this later). The latter part of the term, "host-based", means that it runs on a network host or computer, as opposed to being a standalone or separate appliance. Of course there are several other types of firewalls in existence, but a discussion of their pros and cons falls outside the scope of this paper.[5]

Some features and configuration options of WF include:

- Enabling static exceptions for ports
- Enabling exceptions for applications (useful when an application's port number requirements are not known in advance)
- Configuring basic ICMP options (whether or not to respond to ICMP echo requests, timestamp requests, etc.)
- Logging of dropped packets and successful connections
- Boot-time protection (enforced through a mandatory, unalterable policy which only allows the computer to perform basic networking tasks such as DHCP, DNS, and contact with a domain controller. Once the firewall service has been successfully loaded, the boot-time policy is rescinded).
- Option for configuring all network interfaces using global settings, rather than configuring each one independently
- Port restrictions such that when a port is opened, the user can specify what sources of traffic are allowed (local subnet only, specific IP addresses, specific subnets, etc.)
- Ability to be configured globally via Group Policy
- Command-line configurability using the **netsh** command
- Ability to immediately disable all configured exceptions with a single click (this is referred to as "On with no exceptions" mode)
- Ability to have multiple profiles- for example, one profile for the corporate network, and one for the public internet[6]

ZoneAlarm Firewall

ZoneAlarm, a personal firewall product which is available from several websites (including http://www.zonelabs.com and http://www.download.com), probably has the largest installation base of all the third-party personal firewalls. ZoneAlarm is available in several flavors, with varying levels of functionality. However, at the time of this writing, the latest **free** version is 5.1.033, which is the one we will focus on in this paper.

[5] For more info on firewalls, see http://www.windowsitlibrary.com/Content/121/10/toc.html

[6] Entire bulleted list summarized from pages 27-36 of http://download.microsoft.com/download/8/7/9/879a7b46-5ddb-4a82-b64d-64e791b3c9ae/02_CIF_Network_Protection.DOC

© SANS Institute 2004 Author retains full rights.

ZoneAlarm has many of the same features as Windows Firewall, with the following exceptions:

- It does not feature boot-time protection and kernel integration
- It is not natively configurable through Group Policy
- It cannot be configured locally using the **netsh** command

However, in addition to the standard features of WF, ZoneLabs claims that the free version of ZoneAlarm also provides the following:

- Stealth Mode makes your PC invisible to hackers by default
- Safe Sharing lets you share files and printers safely with trusted people, networks, and subnets
- Program Control ensures that only applications you trust access the Internet
- "Spoofing" Protection prevents hackers from pretending to be you and shutting off your firewall
- Hardened Defenses means ZoneAlarm enters safety mode if attacked by hackers
- AlertAdvisor provides expert security advice and information for each security alert
- Easy to Use default settings provide immediate protection for "set and forget" security[7]

In order to demonstrate the effectiveness of ZoneAlarm and WF in a real-world environment, as well as test the validity of each company's respective claims about their product, I decided to put them both through a battery of tests. Generally, penetration testers who are gauging the effectiveness of a firewall product will use a variety of tools, scripts, and exploits to try to find its weaknesses. Since not everyone in information security is a seasoned penetration tester, fortunately there are several websites which offer varying degrees of automated testing. Most of these are nothing more than scripted port scans and exploit tests which are run against your firewall from the outside, while others are specially designed programs intended to be run *behind* your firewall to check for leaks. I put WF and ZoneAlarm through several of these tests, and the results are provided on the next page.

The test was conducted using a single PC with the following specs:

- Compac Evo D510, 2.0GHz, 256MB RAM
- Windows XP with SP2 and all current security patches
- No additional software installed except firewall application

I started with a completely clean install of Windows XP with SP2 from which I created a Ghost image. Once the image was created, I booted the PC

[7] Entire bulleted list gleaned from:
http://www.zonelabs.com/store/content/company/products/xpInfoCenter/faq.jsp

© SANS Institute 2004 Author retains full rights.

and sequentially ran all the tests against WF (with the default configuration), documenting the results. Once the last test was complete, I ghosted the PC back to the original state, installed ZoneAlarm (keeping the default configuration), then proceeded to run the same tests once more, documenting the results. I must confess that I was a bit surprised by some of the findings.

Let's begin with results of the tests which were designed to gauge a firewall's resistance to attack from an *external* source:

1) Shield's Up! - https://grc.com/x/ne.dll?bh0bkyd2

	Windows Firewall	ZoneAlarm
File Sharing Scan	Passed/Stealth	Passed/Stealth
Common Ports Scan	Passed/Stealth	Passed/Stealth
Advanced Port Scan	Passed/Stealth	Passed/Stealth
Exploits Test	Passed/Stealth	Passed/Stealth
Total Visual Alerts	0	0

2) PCFlank - http://www.pcflank.com/

	Windows Firewall	ZoneAlarm
Quick Test	Passed/Stealth	Passed/Stealth
Stealth Test	Passed/Stealth	Passed/Stealth
Advanced Port Scanner	Passed/Stealth	Passed/Stealth
Exploits Test	Passed/Stealth	Passed/Stealth
Total Visual Alerts	0	83

3) AuditMyPC - http://www.auditmypc.com/freescan/scanoptions.asp

	Windows Firewall	ZoneAlarm
Firewall Test 1	Passed/Stealth	Passed/Stealth
Firewall Test 2	Passed/Stealth	Passed/Stealth
Total Visual Alerts	0	5

4) HackerWatch - http://www.hackerwatch.org/probe/

	Windows Firewall	ZoneAlarm
Simple Probe	Passed/Stealth	Passed/Stealth
Port Scan	Passed/Stealth	Passed/Stealth
Total Visual Alerts	0	4

5) DSL Reports - http://www.dslreports.com/scan/

© SANS Institute 2004 Author retains full rights.

	Windows Firewall	ZoneAlarm
Probe	Passed/Stealth	Passed/Stealth
Total Visual Alerts	0	10

6) Sygate Online Services - http://scan.sygatetech.com/

	Windows Firewall	ZoneAlarm
Scan	Passed/Stealth	Passed/Stealth
Total Visual Alerts	0	5

7) Test My Firewall - http://www.testmyfirewall.com/

	Windows Firewall	ZoneAlarm
Firewall Test	Passed/Stealth	Passed/Stealth
Total Visual Alerts	0	0

As you can see, WF was clearly able to hold its own against ZoneAlarm in these tests, the only difference being that WF of course displayed no visual alerts to indicate that a scan or simulated attack was occurring. While this feature of ZoneAlarm can quickly become rather annoying, it's nice to at least have the option to enable it in certain situations.

Now that we have a fairly good degree of confidence that the default configurations of both firewalls will yield approximately the same protection against attacks from the outside, we can move forward with the remaining tests, all of which test a firewall's resistance to *internal* attacks (or simply requests for network access). These tests are commonly referred to as "leak tests", and they all employ different techniques for breaking through a firewall's internal defenses. The ability to successfully defend against these types of attacks is the hallmark of a well-designed firewall.

1) LeakTest - http://grc.com/lt/leaktest.htm

This test involves downloading a special program from the author's website which can be used to initiate a bogus FTP session. This is not a *legitimate* session because there is no transfer of meaningful data, and the server on the other end is not truly an FTP server- it is only acting as one for the purposes of the test. At any rate, the purpose of the program is to demonstrate the behavior of an installed firewall in the event that a rogue program attempts to initiate an outbound connection. As expected, WF did not complain at all when the LeakTest application was put through the motions, which means that it officially failed the test. ZoneAlarm, however, displayed a visual alert when the LeakTest application ran, which means that it successfully intercepted the unauthorized network access attempt, and therefore passed the test.

© SANS Institute 2004, Author retains full rights.

LeakTest, however, was initially used to demonstrate a much more serious weakness in many firewalls- the inability to differentiate between a hacked or trojaned executable and the real one. Simply renaming LeakTest.exe to the name of a "trusted" application would produce a scenario where the firewall's defenses were useless—the firewall would simply assume that the renamed application's request to access network/internet was legitimate. This weakness has been fixed in the vast majority of personal firewall products today, and as mentioned above ZoneAlarm did successfully defend against this attack in testing. WF, since it does not monitor outbound access attempts, was completely oblivious to what was going on.

Steve Gibson, the author of LeakTest, asserted in 2001 that ZoneAlarm stood alone among the leading personal firewalls thanks to one very important distinction-- it creates a hash of all the programs which are secured for network/internet access, and uses this hash value to verify the identity and integrity of any application which subsequently requests access to the network. Hence, the author of LeakTest proffered the assumption that since ZoneAlarm was the only personal firewall which successfully defended against LeakTest, it was therefore a more secure firewall than the competitors.[8] In recent years, however, most firewall vendors have modified their products to include detections for this type of exploit.

2) TooLeaky - http://tooleaky.zensoft.com

Once word got out about LeakTest (see #1 above), many began to assume that ZoneAlarm was infinitely more secure than its competitors. However, a few clever programmers soon began to realize that the methods used by LeakTest could be "improved" upon, and that ZoneAlarm wasn't quite as impervious as previously thought.

TooLeaky is a program written by Bob Sundling to demonstrate how ZoneAlarm (and any other firewall which relies on a list of "trusted" applications to determine outbound access privileges) can be rendered completely useless by anyone with the most basic of programming skills. TooLeaky can defeat firewalls by essentially making specially crafted program calls to any application which is listed as "trusted" or "allowed" within a firewall's configuration. TooLeaky first locates the Internet Explorer executable (ieplore.exe) on the hard drive, and then it issues a special program call directly to IE, causing a browser window to be spawned off the screen and out of view. When Internet Explorer, a "trusted" application, now asks for outbound internet access, the firewall doesn't complain. Within this browser window, a URL (or potentially any code of the programmer's choice) runs with the full privileges of the browser.

During testing, data was successfully requested and retrieved from the grc.com website without any complaints from WF or ZoneAlarm, proving that a Trojan author could easily get around a firewall's defenses using this method or something very similar.

[8] Results posted at http://grc.com/lt/scoreboard.htm

© SANS Institute 2004 Author retains full rights.

3) YALTA - http://www.soft4ever.com/security_test/En/index.htm

YALTA is yet another program which must be downloaded from the author's website and run locally. This program allows you to direct UDP packets to any IP address across any port in order to test a firewall's ability to filter outgoing traffic. The results were identical to LeakTest's for both the standard test and the "renamed executable" test – WF failed, ZoneAlarm passed.

4) FireHole - http://keir.net/firehole.html

FireHole is a proof-of-concept application much like TooLeaky in that it piggybacks on an application which is invariably "trusted" on the vast majority of PCs with a personal firewall- Internet Explorer. Upon execution, FireHole creates a DLL file on-the-fly which is subsequently loaded into the address space of IE. Since IE is trusted by the firewall, no red flags go up, and FireHole is allowed to run its scripted routine. The author claims that FireHole is more flexible, and therefore potentially more dangerous than TooLeaky. Neither ZoneAlarm nor WF detected that anything unusual was going on during testing.

5) Atelier Web Firewall Tester - http://www.atelierweb.com/awft/download.htm

The Web Firewall Tester application from Atelier combines six separate methods of bypassing firewalls in one application[9]. Both ZoneAlarm and (of course) WF failed all six tests, receiving a score of zero out of ten. According to the Atelier website, "if your Personal Firewall scored less than 10 points you may be able to adjust some settings to improve its performance." However, since most users of personal firewalls don't dig very deeply into the available settings and configuration options, chances are very good that the vast majority of users are vulnerable to all of the exploits demonstrated by the Web Firewall Tester application.

There are countless additional "leak test" applications available on the internet which will demonstrate even more methods of defeating personal firewalls' outbound security. For the purposes of this paper, however, I think it has been sufficiently demonstrated that WF and ZoneAlarm's respective default configurations offer little protection against most of these attacks.

If you would still like to do some additional testing, below is a list of some of the better firewall exploit applications not covered here. Be forewarned, though that running these applications on anything other than a test computer in controlled environment is highly discouraged.

[9] See http://www.atelierweb.com/awft/index.htm for an explanation of the 6 methods

© SANS Institute 2004 Author retains full rights.

- pcAudit - http://www.pcinternetpatrol.com/page/view/49
- Thermite - http://perso.wanadoo.fr/jugesoftware/firewallleaktester/eng/leaks/thermite.exe
- Copycat - http://mc.webm.ru/copycat.exe
- pcAudit - http://www.pcinternetpatrol.com/
- WallBreaker - http://www.firewallleaktester.com/leaks/WallBreaker.exe

The tests which WF and ZoneAlarm were put through clearly demonstrated that both products are more than capable of defending against external attacks. It was equally clear, however, that they are both very susceptible to certain types of internal attacks. As such, it is next to impossible to wholeheartedly recommend either product as a "set it and forget it" solution. However, the original criteria which were established in Section One for the ideal personal firewall solution were:

1) easy to obtain and install
2) comes pre-hardened and pre-configured with an effective rule set offering maximum security
3) is very low-maintenance

Judging strictly by these criteria in conjunction with the test results, I feel that both WF and ZoneAlarm satisfy #1 above. However, they both fail at #2, regardless of how obscure the proof-of-concept applications may be, or how likely or unlikely each test scenario might be played out in real life. If the holes are truly that wide, and it appears that they are, then it's only a matter of time before exploiting those holes and utilizing those same techniques becomes all too commonplace (assuming we are not there already). While some may be satisfied to take that risk and choose to believe that since they are *relatively* secure in this scenario that they needn't concern themselves further, the criterion clearly stated "an effective rule set offering maximum security". I do not feel that either firewall product in its default configuration truly exemplifies this stipulation.

As far as #3, I would imagine that WF probably has the edge here, although its low-maintenance operating mode comes at the cost of inferior protection (this is somewhat reminiscent of the inversely proportional relationship between convenience/availability and security). Alas, we will learn more about some of the configuration and maintenance pitfalls of each product in Section 3, and we can make a better informed decision at that time.

Some may think that combining firewalls (i.e. using WF and ZoneAlarm in tandem) will provide sufficient protection against some of these attacks, whereas either one of them alone would not. This is flawed thinking, since you'd still really only have one firewall (ZoneAlarm) doing any kind of outbound filtering, and we've already seen that ZoneAlarm in its default configuration can be easily compromised. Some others may be inclined to think that a file integrity checker might provide protection in some of these situations, but again- many of these attacks involve launching a "trusted" application, which means that the file integrity of the executable would be perfectly intact. It would seem that the only

© SANS Institute 2004 Author retains full rights.

real defense might involve a super-intelligent virus scanner which either had built-in signatures for the "trojaned" executable, or had excellent heuristics abilities. Given the predominantly reactionary stance of most modern antivirus products, however, this too seems unlikely.

So what options *are* available to users of these products, given the weaknesses they clearly possess? Are we to just sit back and let the "bad guys" ransack our computers and take what they want? Of course not! Even if we can never truly achieve perfect security (is there such a thing?), at the very least we can make it prohibitively difficult for unauthorized users to breach our defenses. The answer lies in hardening the default settings of both firewalls, and of course incorporating them both into a broader defense-in-depth strategy. In Section 3 we will explore some techniques for accomplishing just that.

SECTION 3

Firewall vendors are, after all, businesses, and as such they are keenly interested in delivering products which achieve an acceptable balance between protection and compatibility with other programs. As a result, the default settings which come preconfigured in most firewalls do not typically provide the maximum protection available. It takes a bit of poking around in menus and property pages to really get the most out them. In this section we will examine some of the installation and configuration options for WF and ZoneAlarm, and identify the proper place of each in a multi-layered defense.

In lieu of a detailed, exhaustive analysis of all the possible configuration options for each firewall, complete with screenshots (isn't that what product manuals[10] are for?), let's assume that you've got one or both products already installed and in their default configurations, and simply move on with some of the recommended tweaks and settings changes.

Windows Firewall

There aren't many configuration options available for WF in general, and the default configuration provides decent protection against most external threats. However, there *are* a few things you can do to improve WF's overall security. First off, you should devise a plan for ensuring that the Windows Firewall/Internet Connection Sharing service remains running and isn't accidentally or intentionally disabled. You can accomplish this in a number of ways-- one of the easiest is to configure the service to automatically restart itself if it fails. Simply open up your Services snap-in (go to Start->Run and type services.msc). Double-click on the service to bring up its property page, and go to the Recovery tab. Where it says "First failure", change "Take no action" to "Restart the service". You can do the same thing for "Second failure". For "Subsequent failures", you'll want to do choose something different, such as "Run

[10] **ZoneAlarm Manual:** http://download.zonelabs.com/bin/media/pdf/zaclient51_user_manual.pdf
Understanding WF:
http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx

© SANS Institute 2004 Author retains full rights.

a Program". When you select this option, the bottom portion of the property page is un-greyed and you can browse for a program executable. Common choices for this executable include scripts and programs which will notify you in some way that the service has failed (i.e. send you an email, text page, visual alert, etc.). There is plenty of documentation on the web for this sort of thing.

As far as configuring WF itself, if you'd like to start from scratch with the "out-of-the-box" default settings, Microsoft has provided a quick and easy way for you to do so. Just launch your Windows Firewall configuration applet, go to the Advanced tab, and click the button near the bottom which says "Restore Defaults". After you do that, the very first thing you'll want to get rid of is the built-in exception for Remote Assistance (why in the world would Microsoft enable this by default?). You generally want to have as few exceptions as possible, preferably none for maximum security. Only enable what you absolutely cannot live without.

The final thing you'll definitely want to do is enable logging, so that you can monitor the traffic which is being directed at you. You should periodically (the more often the better) take a look at your logs to see if there is anything you need to adjust. You can also choose to store your log files in a location other than the default (C:\Windows\pfirewall.log) by going to the Advanced tab on WF's Control Panel applet. And while we're on the subject of log files, instead of relying on good ol' Windows Notepad for log viewing, try one of these tools:

- FireLogXP (freeware) - http://www.2brightsparks.com/assets/software/FireLogXP_Setup.zip
- XP Firewall Log Reader (freeware) - http://home.online.no/~msols/XP_Log_Reader.zip
- FirePanel XP (time-limited free evaluation, shareware $10) - http://router19.org:8080/FirePanel%20XP.zip
- XP Firewall Viewer - http://www.download.com/XP-Firewall-Viewer/3000-2085_4-10305656.html?tag=lst-0-1

If upon examining your log files you suspect that your computer may be under some sort of attack, or if you ever need to quickly go into "stealth mode", you should definitely familiarize yourself with "Don't allow exceptions" check box on WF's main property page. If you check the box and then click OK, any exceptions you have previously defined will immediately be deactivated and no unsolicited traffic will be allowed in. This feature is also useful in the event that you transport your computer or laptop to an untrusted or foreign network.

That's really just about it when it comes to locking down WF. There aren't any more firewall-specific settings you can change to extract any more security from it. It's obviously not the most robust firewall, but it gets the job done in a pinch. I have seen several websites which recommend disabling WF altogether in favor of a 3rd party solution. While at first this may seem reasonable due to WF's very limited feature set, I have to say that I disagree with this approach, because for all the features WF lacks, it still has one potential benefit that none of the others can offer: boot-time kernel-mode protection. Not only will this feature

© SANS Institute 2004 Author retains full rights.

protect against any attacks during bootup, but since it is so tightly integrated with Windows, it means you are much less likely to see the dreaded BSOD when the real firewall kicks in. I have personally witnessed things like spontaneous reboots and other anomalies with competing firewall products. So my recommendation is to leave it enabled unless you are also behind a hardware firewall, packet inspection/filtering device, or home-office router, or you are proficient enough with firewalls to truly know what you are doing.

ZoneAlarm Firewall

Since ZoneAlarm actually has its own install routine (as opposed to being automatically installed as part of a larger Service Pack, as in WF's case), the configuration actually begins during the setup process. These settings can be changed once the installation is complete, of course, but it makes sense to get the most secure settings in place as soon as possible- especially in the case of an unprotected internet-facing computer. So let's take a look at some of the more critical configuration options which appear during setup:

1. One of the first options you'll have is to choose an installation directory. It may at first seem an insignificant security measure, but consider changing the default installation directory to somewhere different. Although "security by obscurity" is probably the absolute weakest way of securing something, doing this could potentially prevent a Trojan or malware from successfully locating and disabling ZoneAlarm down the road.
2. When the option to start ZoneAlarm appears, go ahead and allow it to start. As stated before, the sooner you have protection in place the better.
3. When you are asked whether or not ZoneAlarm should display a visual alert when incoming traffic is blocked, choose to disable this feature. While this may seem like a bad idea, understand that a tremendous number of visual alerts can potentially be generated by this setting, and you will be pulling your hair out from all the interruptions. Instead of relying on these incoming traffic alerts to keep you informed, a much better practice would be to disable alerts here and instead monitor your logs very carefully. Even if a Trojan made its way onto your system with the incoming alert option disabled, an alert would still be generated whenever the Trojan attempts to "phone home" for additional instructions or code.
4. The last important setting you'll see during setup is when ZoneAlarm asks you if it's okay to pre-configure program access permissions. In other words, do you want to be alerted each time a program attempts to access the network/internet, or do you want ZoneAlarm to automatically approve access attempts at its discretion? I'm sure you already know the answer to this question. Choose the option which says "No. Alert me later when my browser and these components need internet access."

© SANS Institute 2004 Author retains full rights.

Like WF, ZoneAlarm is a stateful host-based firewall, but as seen in #4 above it also has a limited awareness of activity on the application level. In other words, it provides basic monitoring of applications and network/internet access attempts as an added measure of security. In truth, this is the heart of ZoneAlarm, and you should definitely keep this important feature in mind and use it to your advantage. Generally, ZoneAlarm's default settings will put you a favorable position with respect to security (assuming you chose the right options during setup). However, just as a simple checklist, you'll want to be sure the following settings are in place at all times:

1. In the **Overview** section
   a. Preferences tab – Ensure that "Load ZoneAlarm at startup" and "Protect the ZoneAlarm client" are both selected.
2. In the **Firewall** section
   a. Main tab – Ensure that Internet Zone Security is set to "High", and that Trusted Zone Security is set to "Medium" or "High", depending on whether or not you have a local LAN. "High" is of course recommended. Click the Advanced button, and ensure that "Allow uncommon protocols at high security" is unchecked. This will disable any non-standard protocols which might be used by a Trojan to circumvent your firewall. Also, ensure that "Lock host file" is selected for similar reasons.
   b. Zones tab – Here you should define specific IP addresses or ranges of trusted machines/printers which may reside on your local LAN. Otherwise leave everything blank.
3. In the **Program Control** section
   a. Main tab – Ensure that the Program Control slider is set to "Medium" or "High". You can get away with Medium if you are using WF and ZoneAlarm together.
   b. Programs tab – This is where you'll want to spend most of your time monitoring which programs have been secured for network/internet access. Be extremely selective when granting a program unrestricted outbound or server access- don't grant permission just because it asks. In about 90% of cases, programs don't truly need unrestricted access to function. Most of the time they are just trying to do things like check for updates or report anonymous usage statistics to the author. Ensure that almost every program listed here is set to "Ask" permission. This will ensure that you are always prompted before access is granted. One other suggestion: consider using an alternative to Internet Explorer, such as:

      - Firefox (http://www.mozilla.org/products/firefox/)
      - Opera (http://www.opera.com).

      This way, you can set your Internet Explorer access to "Block" or "Ask", and as a result you won't be nearly as vulnerable to many of the internal attacks which were covered in Section 2.
4. In the **Alerts & Logs section**

© SANS Institute 2004 Author retains full rights.

a. Main tab – ensure that Event Logging is turned on, and that Program Logging is set to "High". This will allow you to keep tabs on all program and network access.[11]

Aside from the free version, ZoneAlarm is available in many other flavors, many of which include features such as antivirus capabilities, privacy protection, and more. However, even if you own one of the upgraded "pay versions" of ZoneAlarm, do not under any circumstances allow yourself to think that ZoneAlarm and/or WF are all you need to be secure. A firewall, although supremely important to a computer's overall security, is absolutely not the only component you will need. An in-depth discussion of recommended security items is beyond the scope of this paper, but the following is a bare-bones list of additional items you should seriously consider adding to your security arsenal:

- Antivirus software, properly configured to retrieve regular updates
- IDS software
- File/application integrity monitoring software
- Anti-spyware programs

During the course of this paper we have taken a look at two very popular firewalls, and discovered the strengths and weaknesses of each through a lengthy series of tests. It has been clearly demonstrated that overall, WF firewall is not as secure as ZoneAlarm. However, in WF's defense, Microsoft never intended it to be as feature-rich or robust as competing 3rd party firewalls- the objective was simply to improve the security of millions of computers worldwide without requiring the average user to run out and get a computer science degree to implement it. In this respect, I feel that WF has met the expectations of its designers, and it will at the very least make Windows machines [temporarily] more secure. Microsoft predicts that by the end of November 2004, 100 million users worldwide will have downloaded and installed XPSP2. Let's hope that the vast majority of these users are either leaving WF in it's default "enabled" state, or are at least tech-savvy enough to be running a properly configured, fantastic 3rd party product such as ZoneAlarm.

REFERENCES

Semilof, Margie. "IT pros skeptical of Microsoft's security claims" 04 Nov 2004. URL: http://searchwin2000.techtarget.com/originalContent/0,289142,sid1_gci860936,00.html

[11] The entire section on hardening and configuring ZoneAlarm was based on http://www.markusjansson.net/eza.html

© SANS Institute 2004 Author retains full rights.

"Firewalls – Internet Security Software" Sep 2004. URL: http://www.consumersearch.com/www/computers/firewalls_internet_security_software/

Berlind, David. "SP2's new firewall: Better than nothing, but not good enough" 08 Aug 2004. URL: http://news.zdnet.com/2100-1009_22-5301625.html

Andersen, Starr & Abella, Vincent. "Changes to Functionality in Microsoft Windows XP Service Pack 2 - Part 2: Network Protection Technologies" 15 Sep 2004. URL: http://download.microsoft.com/download/8/7/9/879a7b46-5ddb-4a82-b64d-64e791b3c9ae/02_CIF_Network_Protection.DOC

"Windows XP SP2 Info Center - FAQs" URL: http://www.zonelabs.com/store/content/company/products/xpInfoCenter/faq.jsp

Jansson, Markus. "Firewalls and ZoneAlarm Guide and Tips" URL: http://www.markusjansson.net/eza.html

© SANS Institute 2004, Author retains full rights.