Global Information Assurance Certification Paper

Introduction to Tiny Personal Firewall for Home Computers.

Joseph Crowley

July 22, 2002

Version 1.4

Abstract

Tiny Personal Firewall is a small but powerful firewall. It is powerful enough to be able to do filtering, save to a log, remote management and MD5 signature support, yet is also small enough to be used on your home computer. Today, internet access isn't just a convenience - it's a necessity. Due to the increasing number of people who do their personal banking, shopping, travel arrangements and email over the internet, combined with the increase in viruses, Trojans and malicious software, the need for a personal firewall on your home computer is greater than ever before.

This document will familiarize you with the basics of Tiny Personal Firewall version 2.0, how it relates to operating on your personal computer, as well as how to get it, install it and configure it. It will also provide you with several advantages and disadvantages in comparison to other personal firewall products, such as Zone Alarm version 3.1.291. Throughout, screen shots will be included to provide an easier understanding of the text. This paper is meant to leave the reader with a better understanding of Tiny Personal Firewall and how it can be used to provide firewall security for your home computer.

Background

Tiny Personal Firewall is certified by ICSA Labs.
The objective of ICSA Labs PC Firewall Certification Program is to select products that provide the following services:

- Ability to be installed by a non-expert user
- Ability to support Microsoft Networking capabilities while providing protection
- Ability to support concurrent dialup and LAN connectivity
- Ability to maintain consistent protection across multiple successive dialup connections.
- Ability to block common external network attacks
- Ability to restrict outgoing network communication
- Ability to log events in a consistent and useful manner[1]

The TruSecure company owns ICSA Labs. TruSecure is the publisher of Information Security magazine, a security magazine for news, opinions and

[1] See the URL: http://www.icsalabs.com/html/communities/pcfirewalls/index.shtml

product analysis, and also NTBugtraq, a popular source of Microsoft related security concerns.

Introduction

Tiny firewall software is free for home use, (otherwise you would need to purchase the license) but this is not why you should use it. When evaluating firewalls, price should be considered, but not the only consideration. Just because it is free does not mean it is the best firewall for your computer. What makes software good is if it fits what your requirements are. What are your requirements for security on your home computer? Now would be a good time to list those so you can compare your needs to what Tiny Personal Firewall provides.
Tiny Personal Firewall works only on Windows: Windows 95, 98, NT and 2000. Microsoft Windows is the most popular operating system for home users. As such, there are a majority of worms, viruses and Trojan horses that target Microsoft systems. These are very strong reasons why you need a firewall on your home computer. The Tiny Personal Firewall program has been around for several years. It has a solid reputation and anyone who wants a firewall for their home computer should like the Tiny Personal Firewall.

Downloading and Installation

There are two ways to download Tiny Personal Firewall version 2.0. The first is to go to http://www.tinysoftware.com/home/tiny2?la=EN click on "Support," then "Products," then on the left choose "Download/Support". Fill out the registration form, then choose Tiny Personal Firewall 2.0 under “Select products” and click “Continue” to download. It can also be downloaded from http://download.com.com/3000-2092-6313778.html?tag=lst-0-1 without going through a site registration process.

Once downloaded, double click on the “pf2.exe” executable.

The first screen you see is Tiny Personal Firewall Setup screen. This is the welcome screen, click on “Next”.

The second screen is the “Choose Destination Location” screen. You have two choices. You can either browse to the location where you want to install it or you can choose the default location. For me the destination location was “C:\Program Files\Tiny Personal Firewall.” If you choose the default location, simply click “Next”.

The third screen is the “Select Program Folder”. You can change the name of the program or leave the name, as it appears, Tiny Personal Firewall. Click “Next”.

The next screen allows you to review your installation options before copying files. Click “Next”.

The last screen is the set up status screen. When completed, it will automatically ask if you want to restart your computer or if you will restart your computer later. Once you have chosen, click “Finish”. I would like to see the reboot process go away and have the program work without a reboot of the system. I also think it is easier for the user to follow along, especially if you are new to firewalls or security. Once you have rebooted, Tiny Personal Firewall is installed.

Configuration

The hardest part of using the firewall software is to configure it.
Tiny Personal Firewall does not adhere to the basic firewall rule: deny all except that which is allowed. If you do not have experience with firewalls, or computer security, then this might be frustrating. Tiny does not have any defaults automatically enabled. By not having any defaults automatically enabled, you are prompted by the firewall every time a packet wants to connect to your computer and every time your computer wants to send a packet out. This part of the Tiny Personal Firewall is probably the most awkward for a person new to security or firewalls.

If we compare Zone Alarm firewall and the Tiny Firewall we will see some differences where Zone Alarm did a better job educating the user and helping the user to make better decisions. Zone Alarm personal firewall has a seven-step tutorial with notes to help guide you and inform you as it walks you through setting up your firewall. The Zone Alarm tutorial can be viewed anytime from the programs folder. I like the ability to use the tutorial anytime. I like not having to access the internet to use a tutorial. Zone Alarm has a better interface and is easier for the user to follow along regardless of your knowledge. What I liked was at the very beginning; Zone Alarm gave a very brief explanation of a firewall. It also explained a basic rule of security. It will block all traffic, incoming or outgoing, unless you specify otherwise. Tiny firewall wants to accomplish this, but it does not do a good job of informing the user, so the user can understand the basics. Unfortunately, Tiny does not help the new user in this area as much as they could. This is very important because just using a firewall does not make you safe. It helps, but if you are comfortable and understand even the basics, then you are off to a good start.

Zone Alarm also has a process where you can choose “More Information”. This feature will provide an IP address. With Zone Alarm after you choose “More Information” if you then choose the Technical Info tab you will see the source IP, source port, destination IP and destination port. I don’t like this feature. If someone is new to security or firewalls, I don’t want them to look up an IP and possibly take it upon themselves to confront the attacker. The "More info."

feature also has the ability to act as an advisor, telling the user if a blocked intrusion is serious, and will inform you about what needs to be done. This is a good feature. Anytime a feature can explain a situation so the user can better understand and be better prepared to make a decision is a plus. Again, if the user is new to security or firewalls, this will help them to understand the risks and what needs to be done. I would like to see Tiny have a feature like this. I would like it to be able to explain to the user what happened, why it is bad and possibly give a website the user can go to for even more information. The more information a user can be exposed to the better, and eventually the user will make smarter security decisions. An example would be when a Trojan tries to get through the firewall. Tiny should alert the user of the intrusion, then the user could maybe get a brief description of what the Trojan does, and perhaps a link to a database at Tiny that the user can visit to get more information. Tiny could update that database daily or weekly of security concerns. The user would have access to a current database of security concerns. This way, the user's firewall would be as current as possible. As it is now, the user does not know how current the database is in detecting Trojans, Viruses and other malicious activity. We are left to just trust Tiny Personal Firewall has the latest security to protect us. However, a basic security principle is to not trust anyone. I would like some reassurance when I use the firewall that I am using the latest version, with the most recent updates, for any new Trojans, viruses or any other new malicious software. I would feel more secure knowing I had the latest database and firewall version.

I would also like to see a basic help system for users to be able to look at answers, without having to go the Tiny website. Especially the first time you are setting up the firewall. You don't want to have to set up filters to get to the Tiny website just to look for answers. It's better for new users to start out on the right path to good security, and for experienced users, it can help reinforce what they want to do. A Frequently Asked Question section that sets up the first couple rules to get a good foundation, before you start to get hit with alerts, would be beneficial. It does not have to be a big FAQ, maybe twenty answers to the most essential or basic questions.

Moving on, I would advise you to put a check in the "Create Appropriate Filter" rule and don't ask again. This will help set up your filter and you can almost seem like you are being walked through this process. After you set up filters, the number of alerts you will receive will lessen. Some advice to think about when setting up your filter would be to limit outbound connections to protocols or ports you are familiar with. Some Trojans, once they get in your computer, will phone back to another computer by connecting to an Internet Relay Chat server while other Trojans will try to capture keystrokes and broadcast them to Internet Relay Chat servers.

Something that should be explained is the definition of a port. Knowing what a port is will help you in your understanding of the firewall. A port is a connection

point for data to enter and exit your computer. When a service or program is started, it will automatically attach itself to the appropriate port. Many ports have specific functions. A short list of common ports might include the following:

Port #
21—FTP—(File Transfer Protocol)
23--Telnet
25—SMTP—(Simple Mail Transport Protocol)
53—DNS—(Domain Name System)
80—HTTP—(Hypertext Transfer Protocol)
137-139—NetBios over TCP/IP
443—SSL—(Secure Socket Layer)
44334—(Tiny Personal Firewall Listening port)

A few ports that you need to be aware of, because they are associated with Trojans or other malicious programs, include:

Port #
6699 and 6700—Napster
12345 and 12346—Netbus
27374—Subseven
31337—Back Orifice

If you receive an alert asking if you want to permit or deny, always deny a program associated with one of these ports.

For people that are experienced in firewalls or computer security, it will be very easy to set up.
This is a good time to remember what your requirements are for your computer.

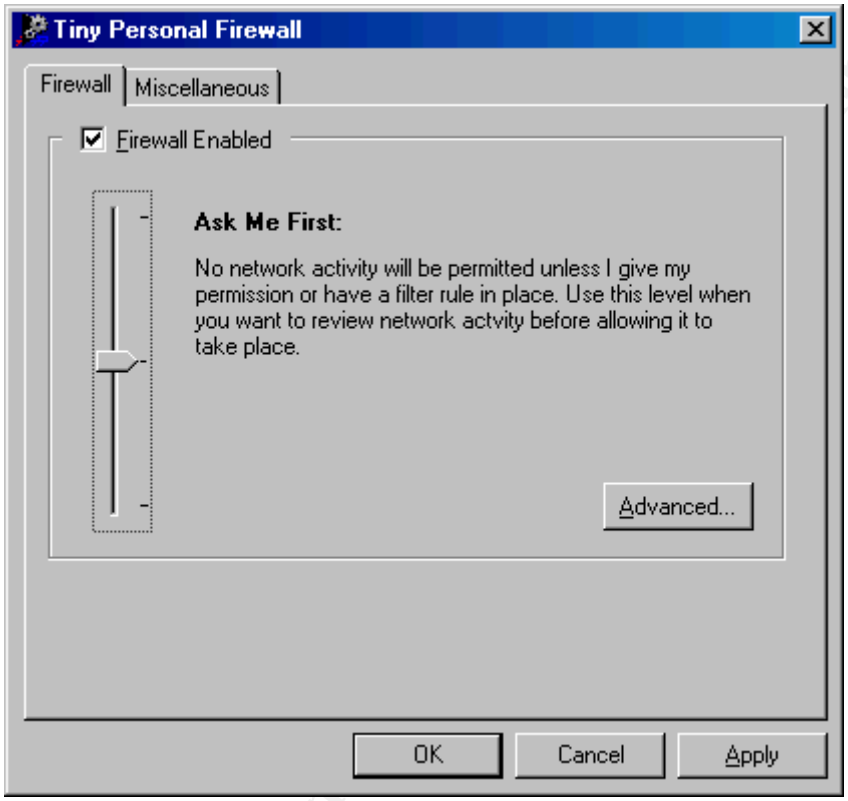
Is remote management important to you?
Do you want to set up a password on your firewall?
Is MD5 signature support important to you?
Do you want some rules to be automatically enabled when the firewall starts?
Do you want to have complete control over your firewall?
Do you want to be able to use a Syslog server? (This would benefit either a corporate user, or someone with more than one computer at home. For more on Syslog, see page ten.)
Do you want to be able to use this with your DSL or Cable Modem?
Do you want to let your children use the computer but also be able to control what sites they can get to?

Next step is to make sure there is a check in the “Firewall Enabled” box.

Under the Firewall Tab, you have three levels of protection on your firewall. Each level explains what type of protection will be enforced.

The first level is "Don't Bother Me".
This will let all packets in and out of your computer. Why would you have a firewall if you did not want to be bothered with packets coming in and out of your computer? The main reason you would choose this option, is if you needed to turn your firewall off temporarily.

The next layer of protection is "Ask Me First".
This is the default setting on the firewall.

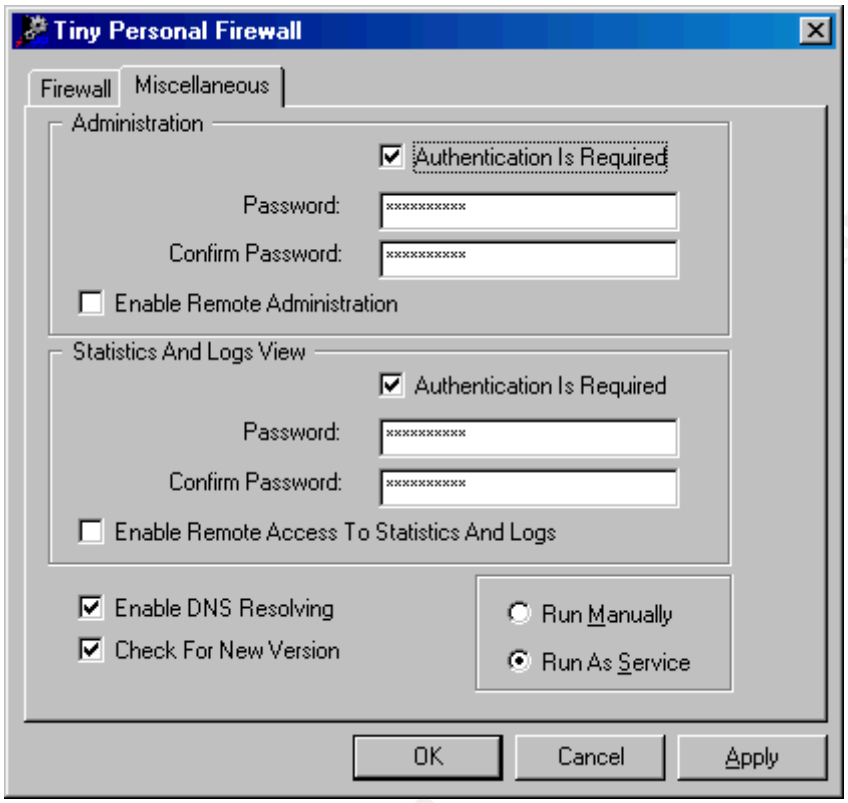


Just like it says, you will be asked every time a packet wants to enter your computer or wants to leave your computer, unless you set up a filter. This is a good feature, as experienced users can set up filters of what they want to allow and deny. For the inexperienced user, this allows them the ability to learn by being asked on every incoming or outgoing packet. This will seem tedious at first, but after a while, the inexperienced user will begin to set up a filter and feel more comfortable using the firewall. This feature works like a wizard in that it prompts you and helps guide you as you slowly learn to set up filters.

The last level is "Cut Me Off".
This will disable all network activity. When you do not need network access this is the level you want. For example, if you have school age children who type reports on the computer, enable this level of protection and you don't have to

worry about them accessing internet chat rooms or other questionable websites. This provides the maximum level of protection.

Now click on the “Miscellaneous” tab.



This is where you would set up passwords for administration, statistics and logs. By default there are no passwords set up. It is a blank password. This is a weak point for Tiny Personal Firewall. It should automatically come with a password as default and it should force you to change the password. You do not want to keep a password that comes with any software. If you were to keep a default password and not change it, then anybody that can attack that software can use the default password as the target, to get into the software. When I looked at the Zone Alarm Index for comparison, I did not see any reference to a password.

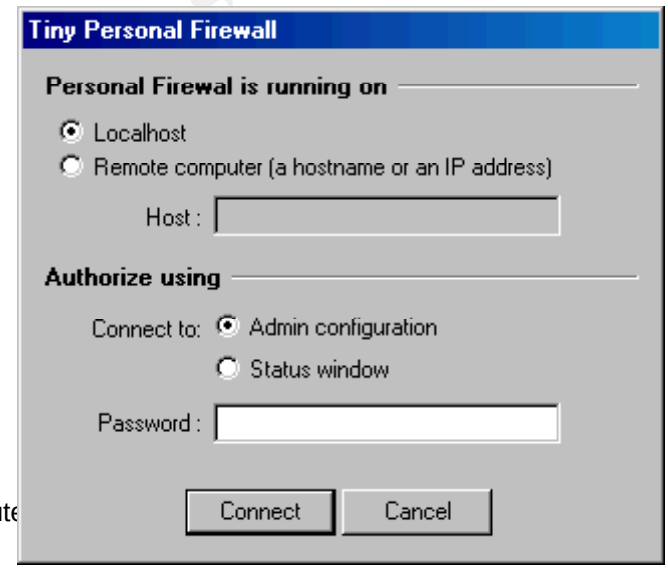
You can also turn on remote administration, which is more for corporate use. Remote administration makes it easier for IT to support telecommuters. This is good for corporate users because it allows IT to monitor, modify and manage the firewall remotely. This way, users don’t need to understand security to get their jobs done. If IT was to install the firewall on a corporate user’s home computer, and that user used their home computer for work, then IT would have a harder time trying to secure and support the firewall. For example, every time

a member of their family wanted to use the home computer to play a game, or if the firewall blocked access, they would be calling IT for support, which you don't want. Also, if the corporate user was using their home computer for work, the IT group would need to verify that computers vulnerability. This is more complex than if the user had a laptop from their office. We want to protect corporate data, and it is harder to do so on a users home computer, than a laptop from work. The Remote Administration feature from Tiny is a good feature. This makes it easier to protect corporate data for IT security.

Tiny also offers "DNS resolving". DNS stands for the Domain Name System. One of its functions is a distributed database that is set up so that when given a hostname, a computer can locate the corresponding IP address. The process of using this distributed database system is called resolving.
This is similar to a telephone directory, in that when given a name, the telephone directory will return the corresponding phone number. Another way to look at this is, if you want to go to a website such as www.abc.com. This will go to the DNS database, look up the name and resolve the name to an IP address. This will, in turn, go to the IP address for www.abc.com.
This helps the computer resolve names and more importantly the firewall will be able to alert you to the port being used, which is generally TCP or UDP port 53.

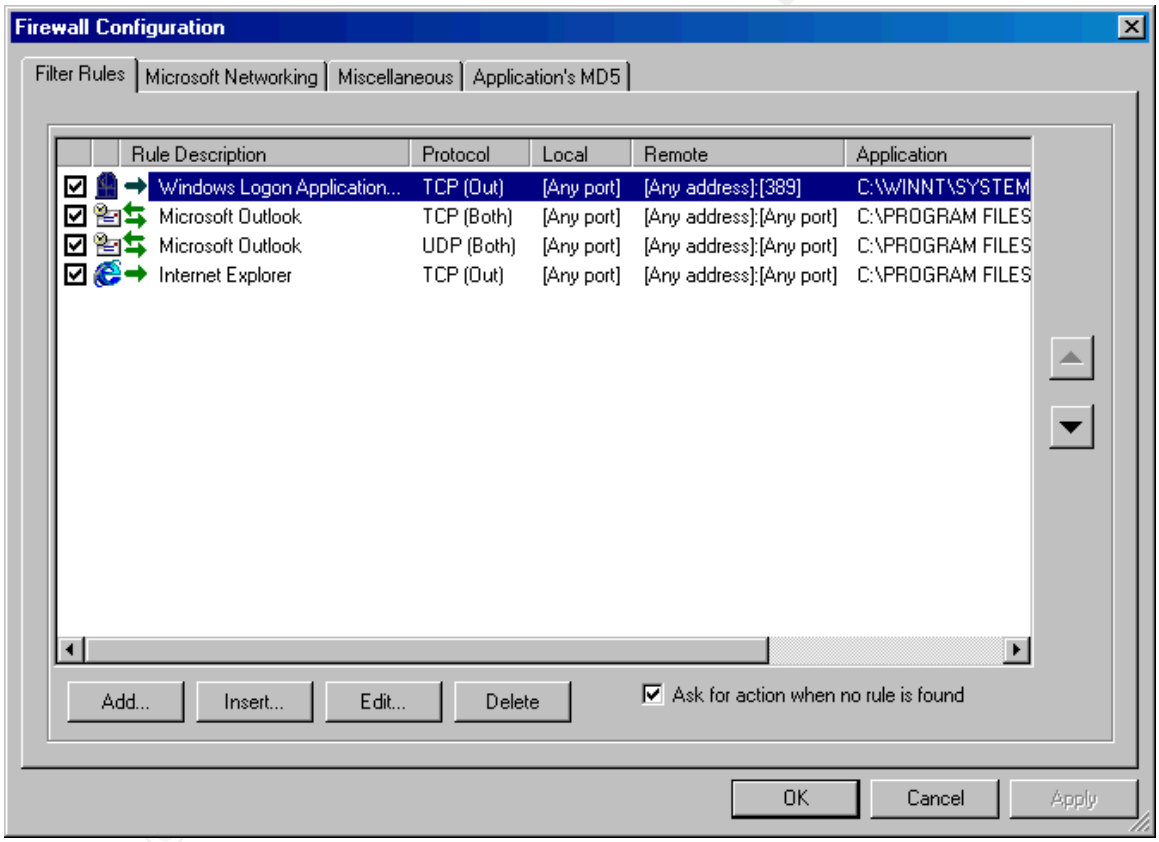
You can also set the firewall up to start as soon as your computer turns on. Choose "Run As Service" and the firewall will always start before any other service starts, when you turn your computer on. This is a good feature as it starts before any application, especially a malicious program like a Trojan horse.

If you set up a password, when you try to access the firewall, you will see a screen that asks for your password. You have two choices: The first option is "Localhost", which is only for viewing the firewall on the local computer. The other option is "Remote Computer", which is where the firewall is installed on a separate computer. With Remote Computer, you can put in either the hostname, or the IP address, for the computer containing the firewall, which will then let you view the firewall from the local computer. The Remote Computer option is good for a company that has many computers the firewall is trying to protect.



Now go back to the Firewall tab and click on “Advanced”.

The first tab is “Filter Rules”. This is a blank screen where you can set up rules and create a filter to either accept packets or deny packets. If you do not set up any rules, it is ok, as this will automatically create the rules for you when you accept or deny packets. What is important to do on this screen is at the bottom right. Make sure there is a check mark next to “Ask for action when no rule is found”. This will always prompt you for action when the computer receives, or tries to send packets, and has no rule already in place. I have created some basic rules in the screen shot below, to show you how the firewall will work in certain situations.

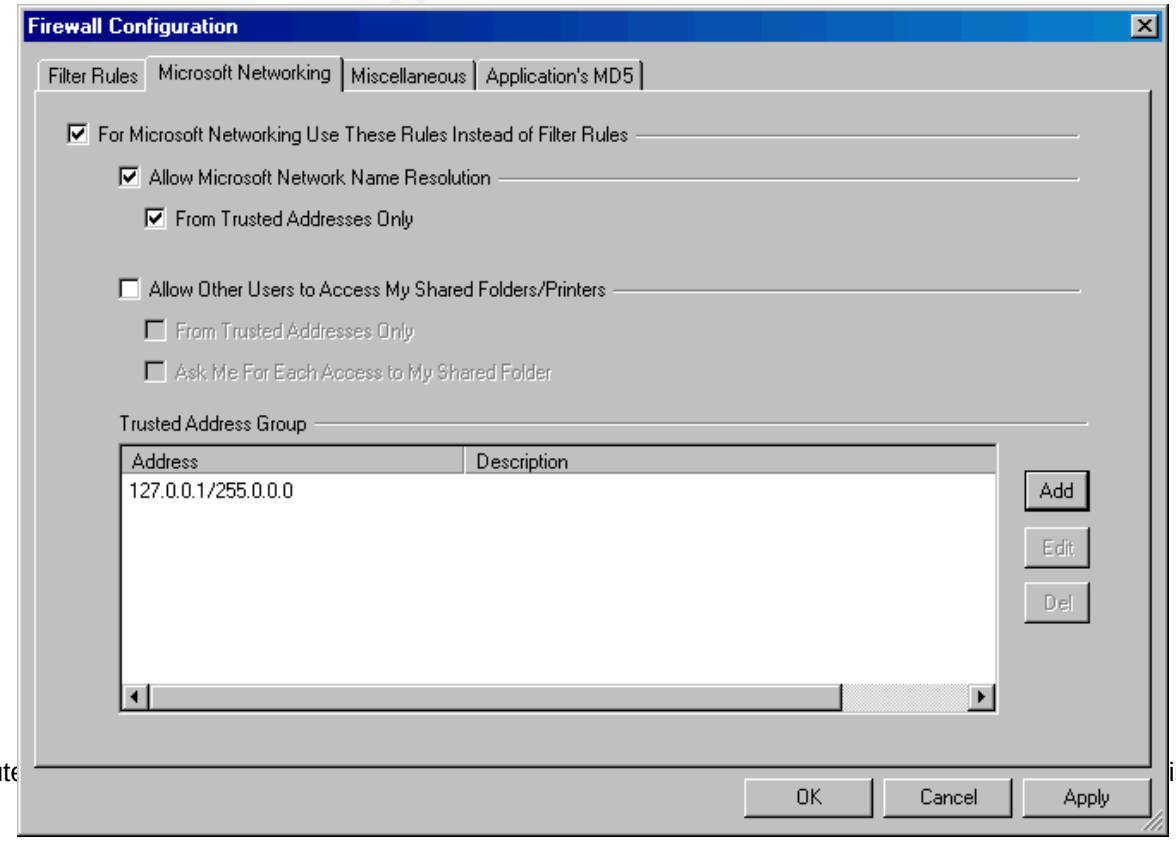


The first rule is for Windows logon. The Protocol is TCP.
The protocols under Filter Rules can be TCP, UDP, ICMP and PPTP.
Local can be used to list the port.
Remote can be used to list the IP address.
Application will list the location of the application, if it is located on your computer, otherwise it will just list the comment Any Application.

There is also an “add” button to add rules to the filter.
“Insert” a rule is similar to adding a rule.
“Edit” or “Delete” are the last buttons you can choose.

On the right hand side of the screen are up and down arrows. I like these, because you now have the ability to set up your rules based on importance. The most important rule should be first, and this will help your firewall efficiency. Highlight a rule, and choose the up or down arrow, and you can move your rules to make your firewall work a little better.

The next tab is “Microsoft Networking”. There are six boxes that you can check to help with your rules. This is where there are separate rules for computers in a Microsoft environment. As you will see, you might not need any of these if you only have one computer at home.
The first box is “For Microsoft Networking Use These Rules instead of Filter Rules”. If you want to use any of the rules, this needs to be checked.
The next box is “Allow Microsoft Network Name Resolution”.
This box will enable your computer to exchange its name with other computers running Windows. If you are using this firewall on your home computer, and you only have one computer at home, then you do not need to use this.
The next box is “From Trusted Addresses Only”. This box will make the Windows name resolution available to a certain group of IP’s. This, too, would only be useful in an environment with more than one computer.
The fourth box is “Allow Other Users to Access My Shared Folder/Printers”.
Below that is “From Trusted Addresses Only”, and the last box is “Ask Me For Each Access to My Shared Folder”.
There is a “Trusted Address Group” screen below that, which will list all the IP’s and subnets in this space.



Now that I have explained what most of those functions are for, let's see how you should configure this if you only have one computer at home. Only select the first option, which is "For Microsoft Networking Use These Rules Instead Of Filter Rules". Leave all other options disabled, as you do not need any communication with a Microsoft network. None of the other options are required for a single computer. This is a good feature if you only have one computer at home. It is easy to configure and, once done, you don't need to do anything with this section unless you add another windows computer at home, and want those computers to communicate.
Zone Alarm has a similar feature for Windows computers. This feature is called local zone. The local zone allows computers you trust the ability to access files on your computer. All you need to do is add the IP's from those trusted computers. This is similar to the way Tiny firewall deals with Microsoft networks, and other computers wanting to communicate with, your computer and access files on, your computer. I prefer the Tiny firewall Microsoft Networking feature because it is easier to configure than the Zone Alarm local zone feature.

The next tab is "Miscellaneous".
Firewall Logging is at the top of the screen.
You can choose "Log into File" (filter.log).
You can also choose "Log Into a Syslog". Syslog was originally used on Unix systems for network, applications and Operating system logging. Syslog is currently a standard Internet Engineering Task Force Request (RFC) 3164. See the following URL for the full RFC: http://www.faqs.org/rfcs/rfc3164.html.

If you are going to use either "Log Into File" or "Log Into Syslog", you will need to remember to choose a log to define where to store the information gathered. This means you need to create a filter to allow logging. I will provide an example of what you need to do to Log Into a Syslog server. Make sure you put a check in "Log Into Syslog" server. I also put a check in "Log Packets Addressed to Unopened Ports". I put the IP of the other computer, which will act as my Syslog server. I wanted my Syslog server to be Windows compatible, since that is how the Tiny Firewall is set up. I used the Kiwi Syslog server Utility software. It was free, but that's not why I chose it. I wanted Windows compatibility, easy to configure and the ability to easily uninstall when I was done using the other computer as a Syslog server. Again, Syslog will only benefit either the corporate user or someone with more than one computer at home. I only wanted to see how this feature performed under the Tiny Personal Firewall. Within minutes of setting this up, I was watching the log fill up with all kinds of information. The log was easy to understand, and listed date, time, a priority level, and hostname. In this case, it listed the hostname for my computer running Tiny Personal Firewall and a message. Most messages looked like this:

Rule ‘Packet to unopened port received’: Blocked: In UDP, an IP Address: port number> localhost: another port number, Owner: no owner

If you set up a Syslog server to collect information you will be amazed at the traffic that tries to get through your firewall.
If you are going to log into a Syslog server then you will need that server’s IP address. A Syslog server is just a server that you will send all information to. It will keep whatever information you want to filter, and have it sent to the server, so you can examine the information to look for trends or possible attacks to your system. Again, this is mainly for a corporate environment, because they will get more attacks than you will. This would be very convenient for a corporate environment, as they can look at the information gathered and be able to see if there is any information they should be concerned about, and also beneficial because the information is not stored on the same computer as the firewall. If an attacker got through the firewall you still don’t want all your information on one computer. Spreading out the information onto a separate server makes it harder for an attacker to tamper with any evidence of what you have accumulated.
For more information on Kiwi Syslog see: http://rr.sans.org/toppapers/kiwi.php

Is your Firewall operating on an “Internet Gateway”? If so, then you would need to check that box. This feature is good to use in combination with Microsoft’s Internet Connection Sharing application. Internet Connection Sharing allows access to the Internet for all local computers using a single IP address. This feature is also for a company or if someone has more than one computer at home. Many users have more than one computer at home and that means the computers will share an Internet connection.

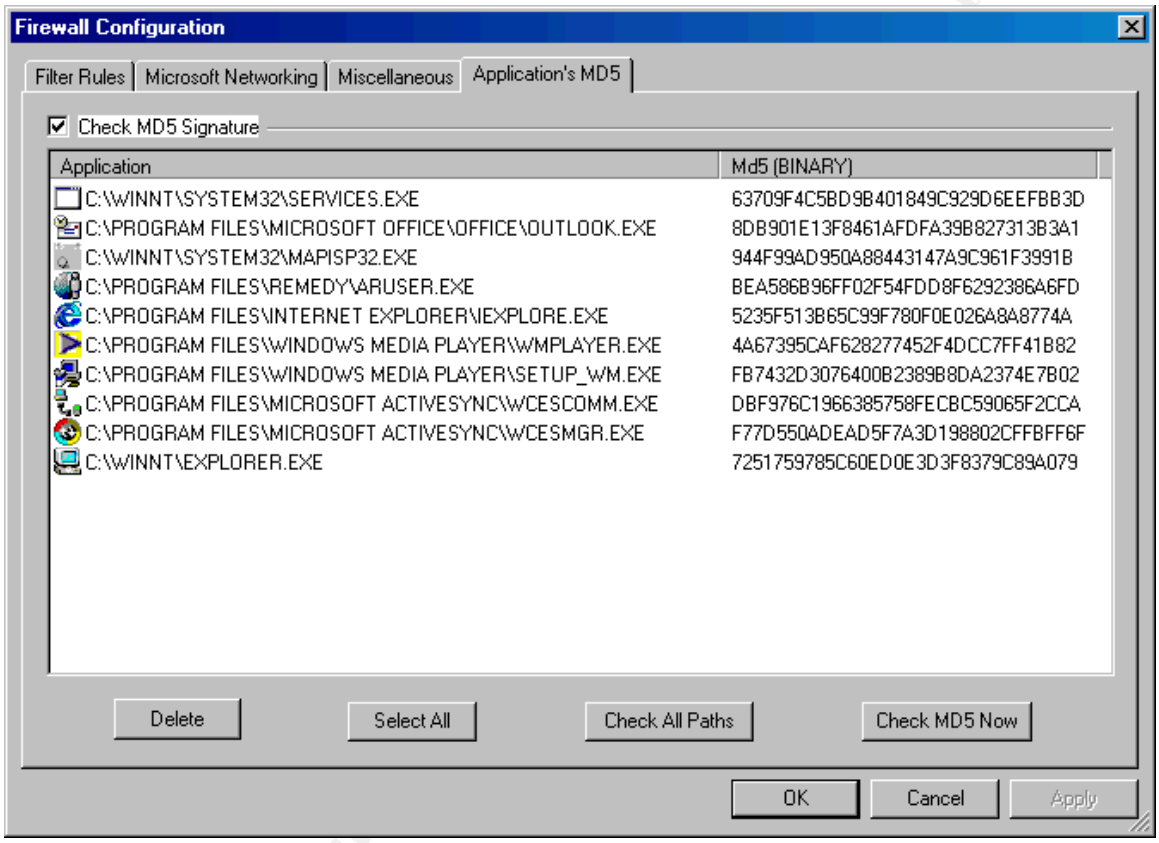
Below that is a custom address group screen.

The last tab is the “Application’s MD5 tab”. This is another good feature of the firewall. Tiny offers the ability to check for MD5 signatures for trusted applications.
MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit fingerprint of an application. Each time an application wants to connect to a certain port, Tiny takes the fingerprint and compares it to the original fingerprint. This makes it almost impossible for an application to be able to duplicate the fingerprint. This means that Trojan horse applications cannot pose as a trusted application.
Before MD5, there was a way to allow Trojans or worms through the firewall. All that was required was renaming the malicious program, such as Netbus, to another program that Tiny firewall recognized by default, like iexplore.exe and then it was allowed to pass through the firewall.
Now, Tiny version 2.0 uses MD5 signature checking, so that even if a program like Netbus is renamed, it’s MD5 fingerprint will still be different and it will not be

allowed through the firewall.

MD5 is currently a standard Internet Engineering Task Force Request (RFC) 1321. See the following URL for the full RFC:
http://www.faqs.org/rfcs/rfc1321.html

Make sure the box is checked “MD5 Signature”.



That’s it for setting up Tiny Personal Firewall.

Summary

Without getting too technical, my goal was to write this paper so that anyone that reads this can follow along, whether they have any security knowledge or not.
After reading this, you should ask yourself why don’t I use a personal firewall? I hope you have a better understanding of why you need one. Having a firewall allows you to control who accesses your computer from the internet. By now, you should be comfortable with Tiny Personal Firewall. I have tried to discuss what you need to know to use Tiny Personal Firewall on your home computer. I also pointed out any areas I thought Tiny Personal Firewall was weak and tried to explain how, on other personal firewalls, those areas were stronger compared

to Tiny. I hope that you realize the flexibility of the Tiny Personal Firewall and also understand a firewall will not protect you 100% of the time. You still need to have anti-virus software on your computer, because firewalls cannot remove Trojans and viruses. With the number of people accessing the internet everyday, even if you have never been a victim of a malicious attack, you probably know someone who has or at least have heard of various Trojans and viruses through the media. Another reason to protect your computer from an attack is that you most likely have some personal information on there.
Lastly, it is only a matter of time before your personal computer is attacked. Protect yourself, and install a firewall before an attacker gets into your computer.

There is an online manual at the Tiny website.
See the URL:
http://www.tinysoftware.com/home/tiny2?s=869876848978968341 7A6&pg=solo_download.
There is also a pdf. Manual you can download.

References

Bahadur, Gary. "Personal Firewalls Under Fire" Information Security Magazine. July 2001. 41-53.
URL: http://www.infosecuritymag.com/articles/july01/cover.shtml

Bigelow, Stephen J. "Tiny Personal Firewall 2.0.14" July 2001
http://www.cnet.com/software/0-352108-8-6549670-2.html

Cole, Eric, Newfield, Mathew, Millican, John. GSEC Security Essentials Toolkit. Indiana: QUE Publishing, 2002. 110-116.

ICSA Labs Firewall Certification Criteria
http://www.icsalabs.com/html/communities/pcfirewalls/index.shtml

IETF MD5 RFC
http://www.faqs.org/rfcs/rfc1321.html

IETF Syslog RFC
http://www.faqs.org/rfcs/rfc3164.html

Langa, Fred. "Langa Letter: Firewall Feedback." Information Week April 15, 2002
http://www.informationweek.com/shared/printableArticle?doc_id=IWK20020412S0009

Markus, Henry Stephen. "The Home PC Firewall Guide" July 2002.

http://www.firewallguide.com/software.htm

Rubenking, Niel J. “Tiny Personal Firewall 2.0” PC Magazine February 2002.
http://www.pcmag.com/article2/0,4149,2047,00.asp

Tiny Software Support Literature and Online support Resources
http://www.tinysoftware.com/home/tiny2?s=869876848978968341 7A6&pg=solo_download

To download Tiny Personal Firewall 2.0.
http://download.com.com/3000-2092-6313778.html?tag=lst-0-1
or
http://www.tinysoftware.com/home/tiny2?la=EN

To download Zone Alarm
http://www.zonelabs.com/store/content/company/zap_za_grid.jsp

Wilkins, Brian R. “Effective Logging & Use of the Kiwi Syslog Utility” June 2002.
http://rr.sans.org/toppapers/kiwi.php