Global Information Assurance Certification Paper

Free Personal Firewalls - Which One Should I Choose?

SANS Security Essentials GSEC Practical Assignment Ver 1.3
David Polano
January 23, 2002

Introduction

Firewall have become an integral part of network security. In the past firewalls were used primarily in large companies that were trying to protect their networks from attack from the Internet. However, with the widespread use of personal broadband Internet access, home users now more than ever need to ensure that they are protecting their systems from attack. The good news is that there are several free firewall products that can do the job. This paper will describe what is considered the top three free personal firewalls for the Windows platform, ZoneAlarm, Tiny Personal Firewall and Sygate Personal Firewall. A common set of criteria will be used to examine each of these firewalls and a recommendation will be made at the end of the paper on which firewall is the best of the three.

Background Information

To ensure that everyone reading this has a basic understanding of how the Internet works, we will briefly discuss the underlying technology of the Internet. The Internet is basically one large network that uses a common set of protocols for communication. Each system on the Internet has as an unique address which allow it to communicate with other systems on the network. The following is a list of terms that you will need to understand in order to be able to successfully configure a personal firewall:

Packet: A packet the basic unit of information that is transmitted over the network. A packet is broken down into many fields which contain things like source and destination addresses, flag settings, sequence numbers, etc. and of course, the data. If the data is too large to fit into one packet, it is broken down into small pieces and fit into several packets.

Protocol: A protocol is a set of rules used to establish communication. In the case of the Internet, the main protocol used is TCP/IP. TCP/IP or Transmission Control Protocol/Internet Protocol is actually two protocols. The IP protocol is responsible for unreliable communication between two points on the network. In other words it looks after the delivery of the packets. TCP is responsible to ensure that the communication is actually completed successfully. TCP will ensure that the packets of information are delivered and received in the correct order. The other two protocols that you need to be aware of are UDP and ICMP. UDP is like TCP however, it lacks the ability to break data into small units and does not provide sequencing of data packets. ICMP is a message control and error-reporting protocol.

IP Address: In order for two points to communicate, each point needs to have a unique address. With the Internet, the address is based on 4 numbers separated by

a decimal points. This is called the IP address. Each of these numbers can range from 0 to 255 however certain numbers in this range are restricted for special purposes. For example, the IP address of the SAN's web site is *209.53.4.130*.

Port: A port is an address on a local system that allows communication between specific applications. You can think of the IP address as the address of your house and the port is like your front door. However, in the case of the Internet, there can be up to 65536 ports (doors) For example, if I wanted to access a web site, I would need to contact the web site's IP address on port 80 (port 80 is the standard port used for HTTP communication). Ports can range from 0 to 65535 with ports 0 to 1024 reserved for specific uses.

Firewalls - The Basics

Before we start looking at these three products, we should spend some time discussing the basic firewall principles so that we are all on the same page. The basic principle of a firewall is very simple, restrict access to one system or network from another system or network. It is a perimeter defense system. A firewall protects your system or network from hostile intrusion thereby protecting your data and systems. A firewall can be implemented in hardware or software and some cases, a mixture of both.

Firewalls fall basically into four categories, *Packet Filters, Circuit Level Gateways, Application Level firewalls and Stateful Multilayer Inspection Firewalls*. A Packet Filter firewall examines each packet as it is received and compares it against a set of rules. If the rules allow the packet to pass, then the packet is allowed to proceed. If the rules don't allow it then the packet is dropped. Circuit Level Gateways work by examining the TCP connection to determine whether or not the session is valid. Application Level firewalls work by examining the traffic at the application level. Because these firewall examine data at the application level they have more knowledge about the nature of the traffic that they are watching. Stateful Inspection Firewalls are a combination of the first three categories. They filter packets at the network layer, ensure that the session is valid and finally evaluate the contents of the packets at the application level.

Many personal firewalls are examples of packet filtering firewalls that also have the ability to monitor network activity at the application level. By monitoring the network traffic at the application level they can ensure that only authorized application are allowed to access the network.

Testing Criteria

In order to compare these firewalls the following criteria was used:

- Installation and Registration Process
- Features
- Default Configuration
- User Interface
- Online network scans using Sygate Online Security Service (http://scan.sygatetech.com/)and Steve Gibson's Shields Up Scanner

(http://grc.com/default.htm)
- Overall Comments

The system used to evaluate these products was a PII 350 w/256 MB of RAM running Windows XP (Home Edition)

Zone Alarm (Version 2.6)

Installation and Registration

ZoneAlarm is a 2.8 MB download from their web site at http://www.zonealarm.com. No registration information is required to download the software. After the file has been downloaded to your system, simply shut down any existing applications and launch the executable (in this case zonalm26zla.exe). The initial install screen allows you to configure the installation location (defaulted to Program Files) and also allows you to select whether or not ZoneAlarm should be configured to allow any web surfing components automatic access to the Internet. The default to this option is set to Yes. The second installation screen prompts you for your name, company and email address. You must provide all the information requested on this page in order to proceed. The options for automatic registration and the option to receive important update news from ZoneAlarm are already selected meaning you are agreeing to both services unless you de select them. If you registering your copy of ZoneAlarm it allows you to download future updates. The third screen is a standard licensing agreement with the usual disclaimers. At this point the installation commences and completes in less than a minute. After the installation is complete, a user survey is displayed and you are asked to complete it. You must complete the survey before you are allowed to finish the installation. After the installation is complete, you are prompted whether or not you want to start ZoneAlarm.

After clicking on OK to start ZoneAlarm, several services are automatically started and a Getting Started Wizard is launched. This wizard will walk you through the basic operations of ZoneAlarm and describe some of the features. This wizard consists of 7 screens and does not require that you input any data. You can exit from the wizard at any time. When the getting started wizard is complete, ZoneAlarm starts and the first ZoneAlarm "tip" is displayed. You can disabled the tips feature by clicking on the "Do not show this message again" option on the tips screen.

Features

ZoneAlarm has the following features:

- Alert logging
- Alert pop-ups. Can auto create persistent rules for application that need access to the Internet from these pop-up windows
- Internet Lock feature. Allows you to disabled your access to the internet with one click of a button. Can also be configured to "lock" after a certain period of inactivity.
- Pass lock feature. Allow you to configure certain application to access the Internet while the Internet lock feature is activated.

- Local and Internet Zones. This feature make it easier to communicate with other systems defined as being part of the local zone. All systems not part of the local zone are automatically consider part of the Internet Zone.
- Program authorization. Can authorize certain application to access the Internet Zone and Local Zone. Records the name, version, file size and creation date of each application to prevent Trojan applications from trying to impersonate legitimate applications.
- Mailsafe features prevent VBS attachments from running on your system.
- Allow Server option. Allows local programs to accept incoming calls from the Internet
- Automatic load on startup
- Automatically checks for updates
- ZoneAlarm tips on startup and shutdown of the Control Center
- Traffic activity indicator to show amount of traffic being upload to and download from the Internet
- Online documentation

Default Configuration

The following are the default setting for ZoneAlarm:

- Alerts are logged and alert pop up windows are enabled.
- Automatic Internet lock is not enabled.
- Local Zone security set to medium meaning that all application must be authorized before they can access the Internet. Computer is visible to local network only.
- Internet Zone set to high meaning that it hides all ports not in use by applications and blocks access to Windows services and shares.
- Web browser authorized to access the Internet (assuming default options were selected during install).
- Mailsafe protection enabled.
- Configured to load up at startup.
- Configured to automatically check for updates.
- No default incoming/outgoing traffic allowed from/to the Internet.
- Blocks ICMP and NetBIOS packets from the Internet.
- Local Zone allows ICMP and NetBIOS packets.

User Interface

ZoneAlarm's interface is clean and easy to use. To start the "Control Center" you simply need to right click on the ZoneAlarm icon in the system tray and select the

Restore ZoneAlarm Control Center option. From this menu you can also engage the Internet Lock, stop all Internet activity and shutdown ZoneAlarm all together.

The Control Center is well laid out and can be displayed in either an expanded or minimized form. The minimized Control Center has large buttons to either enable the Internet Lock or stop all Internet activity all together. The Control Centre is broken down into five main areas: *Alerts, Lock, Security, Programs and Configure*. Each one of these sections is well laid out and easy to understand. The *Alerts* section allows you to examine alerts that have occurred. The *Lock* section displays the lock status and allows you configure the Automatic Lock feature. The *Security* section allows you to configure the security options for both the Local Zone and Internet Zone. From here you can also select the advanced button to add systems to your trusted local zone. The *Programs* section shows the status of all running applications accessing the network. From this screen you can make changes to the properties of these applications. The *Configure* section allows you to modify several options including "on top during internet activity", "load ZoneAlarm at startup" and whether or not you want to be notified before ZoneAlarm exchanges information with Zone Labs Inc.

When you have a new application that needs to access the Internet, ZoneAlarm will pop-up a window asking if you want this application to access the Internet. You can either let the application access the Internet that one time or set it up such that it will always be allowed to access the Internet. When a system on the Internet tries to access a specific port on your system, an alert will be generated and displayed. Your only option is to acknowledge the alert. You can, if you wish, select the option that will prevent these types of alerts from being generated. You can also click on the more information button to get more details in regards to the type of access that was detected.

Online Scanner Tests

Sygate Online Services and Steve Gibson's Shields up did not report any vulnerabilities with default installation. According to both tests, the system was fully protected.

Overall Comments

ZoneAlarm is a good firewall for a user that does not have very much knowledge about firewalls and what they do. The installation is straight forward and they attempt to educate the user before the firewall starts generating alerts. This is a definite plus when it comes to the non technical users. The interface is very non technical and easy to understand. The lack of ability to define specific rules and other advanced operations is a real shortcoming. However, since the product seems to be geared to the non technical Internet user, such features would probably not be useful to this type of person. The Internet lock feature and related options are an excellent addition to this product. The use of two zones is also very useful for allowing one to configure unrestricted access between trusted systems. The online documentation is very thorough and easy to navigate. The Mailsafe feature is an interesting addition to the product however it is only limited to protect against VBS attachments. This is not clear unless you read the documentation and therefore may

be somewhat misleading to some users Even though the logging is useful, to analyze the data you need to be connected to the Internet so that the software can communicate with the ZoneAlarm web site.

Sygate Personal Firewall (Version 4.2)

Installation and Registration

Sygate is a 3.8 MB download from their website at http://www.sygate.com. No registration information is required to download the file. Launching the downloaded file (spf.exe) start the installation wizard that walks you through the installation process. You must agree to the standard disclaimer before you can proceed. The installation defaults to the standard Program Files directory but this can be changed if needed. The wizard prompts you in regards to the placement of the program software icons in the Sygate program group. Again, this can be modified if needed. Installation is very quick and completed within 20 seconds. A reboot is required when the installation is complete. After the reboot, Sygate is automatically started and you are presented with a Registration screen. You have the option of registering immediately or you can opt to register later. In order to receive email support and free upgrades, you need to register and supply a valid email address. Registration requires that you supply your name, company name, title and phone number. After the registration is complete, no further instructions are provide but the Sygate icon now appears in the System tray.

Features

- Many of the most used options are easily available by right clicking on icon in system tray
- Ability to hide Windows services remove unnecessary clutter from applications list
- Provides easy access to online scanning service through Sygate's Online Services web site.
- Application authorization - Allows you to specify which application can access the network
- Advanced application authorization allows you to specify specific IP addresses that an application can access for both local and remote ports.
- Ability to view the connection details of all the running applications
- Ability to schedule when certain applications can access the Internet
- Password protection for firewall configuration.
- Automatically checks for updates
- Email notification of Alerts
- Extensive logging capabilities (Security, System, Traffic and Packet logs). Automatic log turnover (user configurable by size and/or number of days)
- Ability to easily share printer and files on local network and to browse Network Neighborhood
- Ability to block all traffic when screen saver is activated
- Ability to block and/or allow traffic during scheduled times
- Ability to configure advanced rules
- Verifies that application access the network have not be modified or replaced with

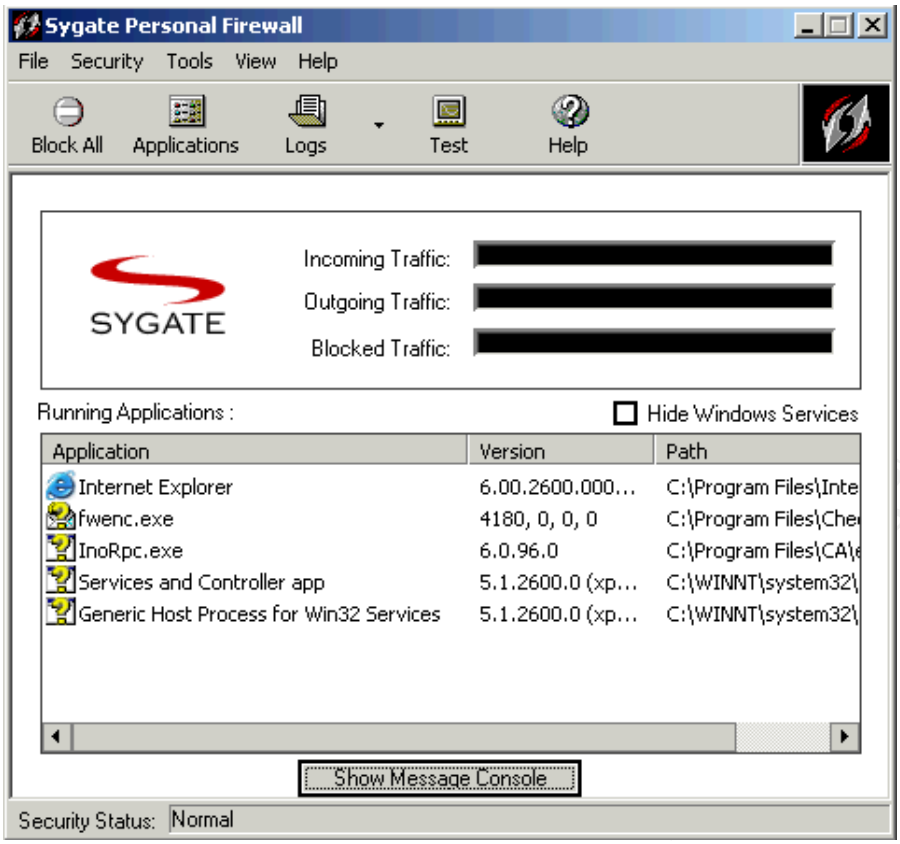
alternate copies (Trojan protection)
- Online documentation
- Detailed alert pop-ups. Can auto create persistent rules for application that need access to the Internet from these pop-up windows.

Default Configuration

Sygate default configuration is as follows:

- No application have access to the network
- Security is set to medium (other options are block all traffic and allow all traffic)
- When an application is authorized to access the network, it is automatically allowed access even when the screen saver is activated.
- Log turn over is set to 512 KB or 30 days
- Packet log is not enabled by default
- Email notification is not enabled
- System allowed to browse network neighborhood files and printers by default.
- Automatic load at startup
- Automatically checks for updates
- Configuration password protection not enabled

User Interface



Sygate's user interface is clean and efficient but is not quite as user friendly as that of ZoneAlarm. The initial screen displays the current traffic (incoming, outgoing and blocked) and allows one to quickly find which running application are attempting to access the network. Simply right clicking on the Sygate icon in the system tray give you access to the various options without having to start the general user interface. The windows used when reviewing or modifying the application allowed to access the network are somewhat small and cannot be expanded. This makes it difficult to view all the columns. The online documentation is quite throughout but not as easy to navigate as that of ZoneAlarm's. The logging capabilities of this product are extensive. Unlike with ZoneAlarm, you don't need to access their web site in order to analyze the logs. The ability to automatically turn over the logs after a specified time frame or after the logs reaches a certain size is a definite bonus compared to ZoneAlarm's logging capabilities. The test button on the menu bar provides easy access to Sygate Online Services web page so that you can run tests against your firewall. The ability to add advanced rules is an excellent option something that was noticeably missing in ZoneAlarm.

Online Scanner Test

Sygate Online Services and Steve Gibson's Shields up did not report any vulnerabilities with the default installation. According to both tests, the system was

fully protected.

Overall Comments

Sygate's Personal firewall is a complete firewall. Even though it lacks some of the easy of use characteristics of ZoneAlarm, I felt it achieved a good balance between usability and rich set of features. This is a firewall that a hard-core technician can use and get the required information out of to make sense of what is happening at the firewall. However, it is not so technical that an everyday user cannot use it. The ability to lock the configuration changes is an excellent feature to ensure that setting are not either intentionally or accidentally changed. The logging capabilities are excellent and easy to navigate through. The logs can be easily sorted and even exported to a file. The ability to email alerts is another excellent feature on this firewall and not available with ZoneAlarm or Tiny Personal Firewall.

Tiny Personal Firewall (Version 2.0.15)

Installation and Registration

Tiny Personal firewall is a 1.4 MB download from http://www.tinysoftware.com web site. This is the smallest download of all three tested firewalls. Launching the downloaded file (tpf.exe) starts up an installation wizard to guide you through the install process. The software installs to the default Program Files directory as expected but you can change this if needed. You also have the option of changing the program folder where program icons will be added. Installation is very quick and completed within 10 seconds. A reboot was required after the install. No registration of any sort is required for either the download or installation of this software.

After the reboot, you are immediately presented a Microsoft Network Setup screen regarding the presence of NetBIOS packets. By default, TPF is setup to allow Microsoft Network Name Resolution to the network attached to the default adapter. No additional information is presented after the reboot.

Features

Tiny Personal Firewall comes with the following features:

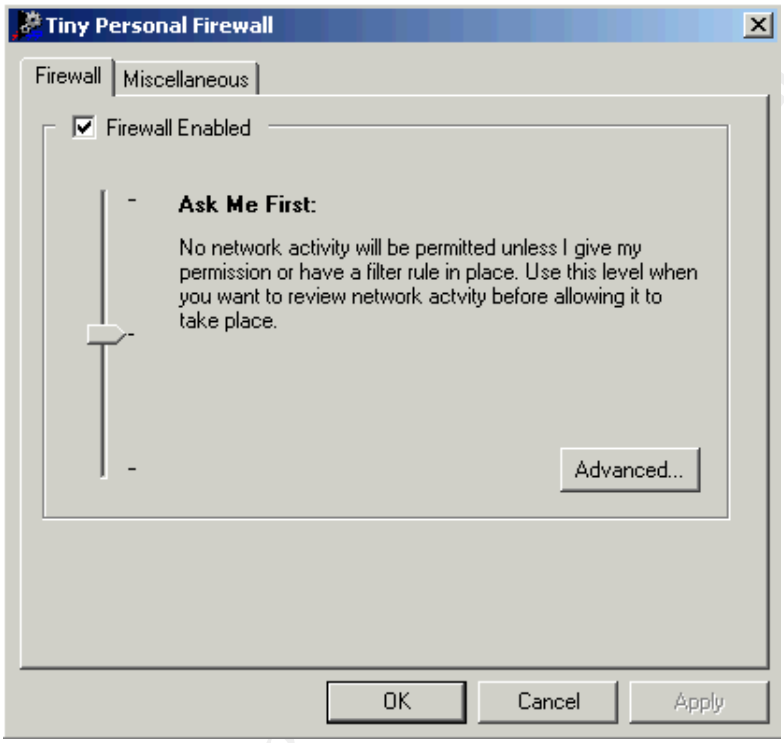
- Remote administration of other TPF clients
- Application authorization to ensure that only authorized applications can access the Internet
- Automatic updates
- Ability to display firewall statistics
- Real time view of running application accessing the network
- Password protection for configuration settings and log viewing.
- Ability to log events to a Sylog server
- MD5 signature verification to ensure application have not be modified or overwritten
- Allows for the creation of advanced rules

Default Configuration

Tiny Personal Firewall default configuration is as follows:

- Configured to load on startup
- Default security setting is set to prompt before an application can access the network
- Default rules for Microsoft network already activated to allow to share folder/printers on trusted network and to allow Microsoft network name resolution
- DNS resolving enabled

User Interface



Tiny Personal Firewalls interface is very basic. This type of interface would be adequate for the technical user but would be somewhat intimating to the every day user that did not have much knowledge of firewalls. To start the firewall administration window, you need simply right click on the TPF icon in the system tray. The initial screen of the administration window displays what the state the firewall is in. There are three options to select from (Cut Me Off, Ask Me First and Don't Bother Me). The other tab on this screen is a miscellaneous tab that allows you to add/remove password for administration and log viewing

The only other option available when right clicking on the system tray icon, is for the Firewall Status Window. The status window will show you a real time list of all running applications accessing the network. Details include the amount of data an application is sending along with transfer speeds, remote addresses and ports. From this screen you can also access the firewall logs. Only a single log is maintained and there is no way to sort or export the log to another file. Also there does not appear to be a way to automatically turn over the log after a certain amount of time or when the log reaches a certain size. An excellent feature that is accessible from

this status window is the ability to remotely manage another Tiny Personal firewall. You can select to either bring up the Administration or Status windows of a remote client.

Online Scanner Tests

Sygate Online Services and Steve Gibson's Shields up did not report any vulnerabilities with the default installation. According to both tests, the system was fully protected.

Overall Comments

Tiny Personal Firewall is a very no frills kind of firewall. The interface is not very user friendly and would be difficult for the non technical person to understand. The default configuration causes TPF to generate many alerts that could be ignore. Such alerts would confuse a user who didn't have a good understanding of what the firewall is trying to tell them. And with complete lack of online documentation, the user is forced to go the Internet to find information on their web site or in one of the various Usenet groups that discuss this particular firewall. This is the only firewall that did not require registration but as a consequence, there is no support of any sort given by the vendor. The logging capabilities of this product are somewhat disappointing and don't come anywhere near the logging feature of Sygate. Two features that really stick out with this product is the ability to remotely manage another TPF client and it use of MD5 signatures to verify that an application has not been tampered with.

Conclusion

Each one of the above firewalls, assuming that it is configured correctly, provides adequate protection for the average home user. Each of the above firewalls passed the two online tests with the default configuration. However from my review, Sygate is the obvious winner. Sygate is a solid firewall and its excellent logging capabilities make it a stand out product. Its only downfall is a lack of up front information to help those users not familiar with firewalls. However, the online documentation can easily bring the non experienced user up to speed.

ZoneAlarm would have to be my second pick. It too is a solid firewall but it does not appeal to the experienced technical user. The lacking ability to create advanced firewall rules is a real disappointment with this firewall. Also, it's logging ability is very limited and requires that you be connected to the Internet if you want to analyze the log information. However, for a user just getting started, this firewall would make an excellent start.

Tiny Personal Firewall has the makings of an excellent firewall but is lacking in several key areas. Firstly, the firewall is geared specifically towards the technical user. And the lack of online documentation makes it difficult for someone to quickly get up to speed. TPF also is lacking in its logging capabilities. It does a better job than ZoneAlarm but comes no where close to Sygate rich set of logging features.

Sygate has proven to be the better of these three firewalls. And since it is available

at no cost, there is no reason for someone not to be using it. Each of the firewalls tested has their own strengths and weakness but in the end Sygate came out on top. It is great to see companies such as Sygate, TinySoftware, Zone Labs Inc. and others coming out with free firewall software. And with availability of other free security software, such antivirus scanners, there is no excuse why users cannot better secure their systems.

Bibliography

Richmond, Robert. "Personal Firewall Comparison." November 4, 2000. URL:http://sysopt.earthweb.com/reviews/firewall/index.html (Dec 29, 2001)

"Firewall Guide Software Reviews" URL:http://www.firewallguide.com/software.htm (January 2, 2001)

Gibson, Steve. "Internet Connection Security for Windows Users." January 2, 2002. URL:http://grc.com/lt/scoreboard.htm (January 10,2001)

"Firewalls Q&A" URL:http://www.vicomsoft.com/knowledge/reference/firewalls1.html*track=internal (Jan 10, 2002)

Comer, E. Douglass. Internetwork with TCP/IP, Volume 1. Prentice-Hall Inc. 1991. 51-82

Bahadur, Gary. "Personal Firewalls." July 2001. URL:http://www.infosecuritymag.com/articles/july01/cover.shtml#f9(January 11, 2002)

Curtin, Matt; Ranum J. Marcus. "Internet Firewalls: FAQ." December 12, 2001. URL:http://www.interhack.net/pubs/fwfaq/#SECTION00030000000000000000 (Dec 27, 2001)

Scher, Rod. "Can You Trust Your PC To a Free Firewall?" June 2001. URL: http://www.smartcomputing.com/editorial/article.asp?article=articles%2F2001%2Fs1206%2F35s06%2F35s06%2Easp&guid=ues29h60&searchtype=&WordList= (January 10, 2002)

VonWald, Michell; Zuk, Nir. "Firewalls Explained." May 10, 2001. http://www.techtv.com/callforhelp/answerstips/story/0,24330,2436994,00.html (Jan 10, 2002)