Free personal firewall for Microsoft Windows®
Comparison chart

By Pierre Szwarc, November 22, 2001.

Zone Alarm® by ZoneLabs	**Sygate Personal Firewall® by Sygate**	**Tiny Personal Firewall® by Tiny Software**
Web site: http://www.zonelabs.com	**Web site:** http://www.sygate.com	**Web site:** http://www.tinysoftware.com
Support: http://www.zonelabs.com/services/support_za_zap.htm	**Support:** news://news.sybergen.com	**FAQ:** http://www.tpffaq.com **Support:** A free **tinyfirewall** Questions and Answers forum exists on http://groups.yahoo.com
Supported operating systems: all 32-bit single-processor versions.	**Supported operating systems:** all 32-bit single-processor versions.	**Supported operating systems:** all 32-bit single-processor versions.
Current version: 2.6.357 (released on October 10, 2001).	**Current version:** 4.2.872	**Current version:** 2.0.15a
Download size: 2,923,120 bytes.	**Download size:** 3,836,595 bytes	**Download size:** 1,416,763 bytes
Internet connection sharing support: yes.	**Internet Connection Sharing support:** yes, Windows 98SE® only	**Internet connection sharing support:** yes.
Virtual Private Networking support: no.	**Virtual Private Networking support:** no.	**Virtual Private Networking support:** yes.

E-mail integrated protection: yes, for one type of attachment (VBS/VBA). Can be turned off in order not to interfere with active anti-virus software.

Inbound protection: yes.

Outbound protection: yes.

Application control: yes (MD5 checksum).

Pre-set rules: yes, hidden and not modifiable.

Configurable global rules: no.

Individual protocol control: no.

Individual port control: no. Global protection levels open or close pre-set ranges of ports.

Individual web site access control: no.

E-mail integrated protection: no.

Inbound protection: yes.

Outbound protection: yes.

Application control: yes (MD5 checksum).

Pre-set rules: yes, hidden and not modifiable.

Configurable global rules: yes. They take precedence over individual application rules

Individual protocol control: yes, in global rules only.

Individual port control: yes. In global rules they can be opened separately for incoming or outgoing traffic. In application rules they are opened both ways.

Individual web site access control: yes, in application rules.

E-mail integrated protection: no.

Inbound protection: yes.

Outbound protection: yes.

Outbound protection: yes (MD5 checksum).

Pre-set rules: yes, modifiable except for local Microsoft networking. The pre-set rules for Microsoft networking can be disabled and replaced by explicit rules.

Configurable global rules: yes. All rules not expressly attached to an application are global.

Individual protocol control: yes.

Individual port control: yes.

Individual web site access control: yes.

?**Trusted" network addresses:** yes. Traffic from these addresses will not be filtered.

Protection settings: three levels for local network and three levels for Internet access, configurable independently. The levels are: Low, Medium, and High. A separate setting (checkbox) is available to enable or disable servers, also for local and external networks.

Intrusion logging: yes. The log includes a link to a Whois function to identify the intruder.

Traffic logging: no.

Content filtering: no.

Network traffic lock: yes.

?**Trusted" network addresses:** yes. Traffic from these addresses will not be filtered.

Protection settings: three global levels: Block everything, Normal, Block nothing.

Intrusion logging: yes. The log includes a Whois and a Traceroute functions.

Traffic logging: yes.

Content filtering: no.

Network traffic lock: yes, through the general level settings.

?**Trusted" network addresses:** yes. These addresses can be used in specific rules. Otherwise they have no special significance.

Protection settings: three global levels: Block everything, Normal, ?Don't bother me".
In ?normal" level, everything not covered by a rule is blocked.
In ?Don't bother me" setting, anything not covered by a rule is let through.

Intrusion logging: yes, rule-based. Each rule can be set to log when matched, and traffic unmatched by any rule can be logged.

Traffic logging: no.

Content filtering: no.

Network traffic lock: yes, through the general level settings.

General remarks: Installation requires administrator privileges on the NT platform (NT 4, Windows 2000 and XP), where it runs as a service. On Windows XP®, requires disabling of the built-in firewall

Uninstallation requires shutting down the service first. Otherwise it will not remove all its files and registry entries, and will interfere with the proper function of the system.

More e-mail protection and finer traffic control is available in the ?Pro" version of this software.

My conclusion

This program is recommended for users who don't have a great knowledge of networking internals.

General remarks: Installation requires administrator privileges on the NT platform (NT 4, Windows 2000 and XP), where it runs as a service. On Windows XP®, requires disabling of the built-in firewall

My conclusion

This program can be set up easily, but offers more control than the default settings for knowledgeable users.

General remarks: Installation requires administrator privileges on the NT platform (NT 4, Windows 2000 and XP), where it runs as a service. On Windows XP®, requires disabling of the built-in firewall

Causes system crashes on multiprocessor systems.

Content and user access control, as well as traffic logging, are available in the WinRoute® router/proxy product line, of which this program is a subset.

Logging control is done per rule, but there is no traffic logging, and interpreting the log requires additional software (available as freeware).

ICSA-certified.

My conclusion

This program offers the finest control over the network traffic. Its configuration is rule-based and requires an adequate knowledge of IP ports and protocols.

Currently this is my favorite personal software firewall.