## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing Lavasoft Personal Firewall</td>
<td>1</td>
</tr>
<tr>
<td> What’s New in Version 2.0?</td>
<td>2</td>
</tr>
<tr>
<td> System Requirements</td>
<td>3</td>
</tr>
<tr>
<td> How to Order</td>
<td>4</td>
</tr>
<tr>
<td>Lavasoft Personal Firewall Interface</td>
<td>5</td>
</tr>
<tr>
<td> The Toolbar</td>
<td>6</td>
</tr>
<tr>
<td> Left and Information Panels</td>
<td>7</td>
</tr>
<tr>
<td> System Tray Icon</td>
<td>8</td>
</tr>
<tr>
<td> Startup Mode</td>
<td>9</td>
</tr>
<tr>
<td> Closing and Stopping the Firewall</td>
<td>10</td>
</tr>
<tr>
<td>Setting the Firewall Policy</td>
<td>11</td>
</tr>
<tr>
<td> Running in Rules Wizard Mode</td>
<td>12</td>
</tr>
<tr>
<td> Running in Background Mode</td>
<td>14</td>
</tr>
<tr>
<td> Running in Entertainment Mode</td>
<td>15</td>
</tr>
<tr>
<td> Running in Self Protection Mode</td>
<td>16</td>
</tr>
<tr>
<td>Managing Applications Network Access</td>
<td>17</td>
</tr>
<tr>
<td> Managing List of Applications</td>
<td>18</td>
</tr>
<tr>
<td> Managing Rules for Applications</td>
<td>19</td>
</tr>
<tr>
<td> Using Macro Addresses</td>
<td>21</td>
</tr>
<tr>
<td>Protecting from Malicious Process Activity</td>
<td>22</td>
</tr>
<tr>
<td> Controlling Application Components</td>
<td>23</td>
</tr>
<tr>
<td> Controlling Penetration Techniques</td>
<td>25</td>
</tr>
<tr>
<td> Understanding Penetration Techniques</td>
<td>26</td>
</tr>
<tr>
<td>Managing Global System Network Activity</td>
<td>29</td>
</tr>
<tr>
<td>Managing Global Rules</td>
<td>30</td>
</tr>
<tr>
<td> Controlling ICMP Protocol Activity</td>
<td>32</td>
</tr>
<tr>
<td> Running in Stealth Mode</td>
<td>33</td>
</tr>
<tr>
<td> Controlling Rawsockets Access</td>
<td>34</td>
</tr>
<tr>
<td>Configuring Local Network Settings</td>
<td>35</td>
</tr>
<tr>
<td> Detecting a Local Area Network</td>
<td>36</td>
</tr>
<tr>
<td> Specifying LAN Access Levels</td>
<td>37</td>
</tr>
<tr>
<td>Protecting Firewall Settings</td>
<td>38</td>
</tr>
<tr>
<td>Preventing Network Attacks</td>
<td>39</td>
</tr>
<tr>
<td>Tracking Network Activity</td>
<td>42</td>
</tr>
<tr>
<td> LogViewer Interface</td>
<td>43</td>
</tr>
<tr>
<td> Left and Information Panels</td>
<td>44</td>
</tr>
<tr>
<td>Creating Multiple Configurations</td>
<td>45</td>
</tr>
<tr>
<td>Contacting Technical Support</td>
<td>47</td>
</tr>
</tbody>
</table>
Introducing Lavasoft Personal Firewall

Being online is fraught with dangers: Internet worms, spyware agents, Trojan horses, hijackers and other malware can wreak havoc, causing anything from slow performance to system crashes and full-blown identity theft. To provide you with the kind of protection you need against cyber thieves and online extortionists, you need a powerful firewall. Your choice in firewalls is one of the most important security decisions you can make. The firewall you choose must be able to monitor all inbound and outbound traffic and protect you from any unauthorized intrusion by rendering your PC invisible to anything that you haven’t specifically authorized.

The award-winning Lavasoft Personal Firewall provides a vastly superior arsenal of defense giving you the latest in personal firewall technology which makes it the clear security choice for your system.

With Lavasoft Personal Firewall:

You know what’s happening on your PC at all times
Lavasoft Personal Firewall watches every connection between your computer and the Internet, alerting you immediately to any communications that may be unauthorized so you can take the appropriate action.

You’re protected by automatic, intelligent protection against hacker attacks
Our Attack Detection plug-in automatically blocks network probes, zombie attacks, and other remote attempts to access your PC.

You control how applications communicate
Component Control and Anti-Leak Control let you decide what applications and processes on your PC are allowed to do and what - if any - outbound connections they may make. Spyware can’t phone home from an -protected PC.

You understand the threats
The Log Viewer lets you review the history of your Internet connections, including sites blocked, attacks repelled, and more than a dozen other security categories that keep you protected, helping you to optimize your protection.

Note:
- For more information about Lavasoft Personal Firewall, please visit http://www.lavasoft.com.
What’s New in Version 2.0?
Lavasoft’s Lavasoft Personal Firewall 2.0 boasts even greater and more proactive security.

The following features are new:

- This version delivers proactive security functionality that blocks all currently-known techniques for bypassing security protection (leak tests), so it fully prevents sensitive data leakage from individual PCs. Its new Anti-Leak Control integrates Hidden Process Control and Process Memory Control technologies available in previous versions and provides a set of additional anti-leak features that prevent such actions of malicious processes as control over another application, components injection, application window control, application launch with command line parameters, and others.

- 2.0 uses a new, ultra powerful Secure Hash Algorithm (SHA) 256 verification routine to identify applications while automatically creating network access rules. This enables to be much more precise in identifying an application in order to ensure the creation and distribution of optimum rule sets. This algorithm replaces the old MD5 algorithm that could be bypassed by recently discovered hacking techniques, which, of course, significantly reduced the ability of this commonly used algorithm to protect users’ machines.

- 2.0 makes it much easier to create the most secure configurations with its new macro definitions for applications and global rules. These can be used, for example, to designate the local network as LOCAL_NETWORK or all DNS servers simply as DNS_SERVERS. This gives advanced users the ability to quickly define security rules for their Intranet communications as well as some Windows-based services (for example, DNS).

- 2.0 also provides a specially designed Entertainment mode that avoids distracting the user’s attention or interrupting a game yet still protects the system when you are playing or watching movies online. While in this mode, the protection is active without bothering the user with numerous prompts or alerts.

- For those who want to decrease the number of prompts, yet still want to have full control, 2.0 suggests the Low level of Component Control, which does not warn about every changed or added application component, but warns only about executable files.

- Finally, 2.0 features a new self-protection mode. With self-protection turned on, protects itself against termination caused by viruses, Trojans or spyware. Even attempts to simulate user keystrokes that would otherwise lead to firewall shutdown are detected and blocked. Also constantly monitors its own components on the hard drive, registry entries, memory status, running services, and so on, and disallows any changes by malicious applications.

Version 2.0 improves overall usability and performance, and is available for 64-bit operating systems.
System Requirements
Lavasoft’s Lavasoft Personal Firewall can be installed on Windows 98/ME/2000/XP or Server 2003 operating systems. The minimum system requirements for Lavasoft Personal Firewall are:

- CPU: 450 MHz Intel Pentium or compatible;
- Hard disk space: 50 MB.

Note:
- Lavasoft Personal Firewall supports 64-bit platforms Windows XP x64 and Windows Server 2003 x64.
- No special network adapter or modem and no special network configuration settings are needed for the normal operation of the software.
- Lavasoft Personal Firewall should not be run with any other firewall software. Running with other firewall products can result in system instability (i.e. crashes) and can cause your system to operate in an insecure mode.
How to Order
Lavasoft Personal Firewall is available for your free evaluation. You are entitled to evaluate the software during the trial period with no obligation to pay. After the trial period, if you decide to keep the software, you must register your copy with us for a small fee.

For pricing information please visit http://www.lavasoft.com/purchase/
Lavasoft Personal Firewall Interface

When you launch Lavasoft Personal Firewall for the first time, its Main Window is displayed. The Main Window is your central control panel of the firewall. Its purpose is to let you monitor network operations of your computer and to modify its firewall settings.

The Main Window is very similar to Windows Explorer; so is familiar to most users making Lavasoft Personal Firewall quite easy to use.

To display the Main Window when it is minimized to the system tray:

- Right-click the firewall’s system tray icon.
- Select Show.

The Main Window contains:

- Menu Bar
  The Menu Bar contains the various commands you can use when working with the firewall.
- The Toolbar
  See The Toolbar section for details.
- Folder Bar
  This displays the name of the tree node currently selected in the left panel.
- Left Panel
  See the Left and Information Panels section for details.
- Information Panel
  See the Left and Information Panels section for details.
- Status Bar
  The Status Bar is the bottommost part of the firewall Main Window. It is used to display the Lavasoft Personal Firewall current state and description of any Toolbar button that you place your mouse cursor over. Also, the current firewall policy is displayed in the right corner of the Status Bar.
The Toolbar

The Toolbar is close to the top of the Main Window. To see what each button does, hold your cursor over it for a second. Each button on the Toolbar is a shortcut to one of the menu items. These buttons are simply an easy and direct path to their functions rather than having to go through several different menus or dialog windows to access the same functions.

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
<th>Corresponding Menu Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Changes a firewall policy.</td>
<td>Options &gt; Policy</td>
</tr>
<tr>
<td></td>
<td>Accesses the Options or plug-in properties dialogs.</td>
<td>Options &gt; General</td>
</tr>
<tr>
<td></td>
<td>Modifies the items a listing is grouped by.</td>
<td>View &gt; Group By</td>
</tr>
<tr>
<td></td>
<td>Narrows a log listing to events within a specified time.</td>
<td>View &gt; Filter By Time</td>
</tr>
<tr>
<td></td>
<td>Enables/disables Self-protection mode.</td>
<td>Tools &gt; Enable Self-Protection</td>
</tr>
<tr>
<td></td>
<td>Opens Lavasoft Personal Firewall Log Viewer that displays the logs.</td>
<td>Tools &gt; Log Viewer</td>
</tr>
<tr>
<td></td>
<td>Displays the firewall’s context help.</td>
<td>Help &gt; Context Help</td>
</tr>
</tbody>
</table>

**Note:**
- Only some of these buttons are visible (active) at any one time, depending on what is highlighted in the Left Panel or the Information Panel.
Left and Information Panels

To display the collected information in a user-friendly manner, Lavasoft Personal Firewall uses two panels. The Left Panel is similar to the left panel of Windows Explorer. It provides a listing of the categories: connections, ports, and plug-ins. The Information Panel gives specific data about any category highlighted in the Left Panel.

As with Windows Explorer, any line that starts with a plus sign (+) can be expanded to show each of its subcategories. Any line starting with a minus sign (−) shows that the line has already been expanded. By clicking on the minus sign, all of its subcategories can be hidden to conserve screen space.

The Left Panel lists and the Information Panel displays the contents of the following categories:

My Internet

Selecting this category displays the welcome screen and information about your current license. It also lists the latest security news from Lavasoft and provides easy access to the Lavasoft Personal Firewall configuration settings. When expanded, this category lists the following nodes:

- Network Activity
  Lists all applications and processes that have active connections and the details of those connections.
- Open Ports
  Lists all applications and processes having currently open ports for a network connection.
- Allowed
  Displays general statistics for all the connections that Lavasoft Personal Firewall has allowed.
- Blocked
  Displays general statistics for all the connections that Lavasoft Personal Firewall has blocked.
- Reported
  Displays general statistics for all the application attempts to access the Internet or LAN that you specified the firewall to report to you (hidden by default).
- Attack Detection
  Displays general statistics for any suspected attacks on your computer from the Internet, the ports involved and where the attacks are from. For information about the Attack Detection plug-in, see the Preventing Network Attacks.

Tip:

- To view detailed statistics, click the Show Detailed Log button in the Information Panel.
System Tray Icon

Another element for controlling the firewall is the system tray icon. The system tray is the rightmost part of the Windows task bar. The blue circle with the question mark is the icon by default. It is displayed right after installing the firewall and is always available as one of the primary ways you can access the firewall controls, settings and logs. The icon changes depending on the current firewall policy.

When you right-click on the system tray icon you get its context menu.

The following commands are available on this menu:

- **Show (or Hide)**
  Displays or hides Lavasoft Personal Firewall Main Window.

- **Show Log Viewer**
  Displays the Lavasoft Personal Firewall Log Viewer.

- **Policy**
  Opens a submenu where you can change Lavasoft Personal Firewall the firewall policy selecting one of the available modes: Disable, Allow most, Rules Wizard, Block most, and Stop all.

- **Options**
  Displays the Options dialog window.

- **Always on Top**
  When selected, keeps Lavasoft Personal Firewall current window on top of all other windows.

- **About**
  Shows the current version of Lavasoft Personal Firewall and lists each module in the package and their version numbers.

- **Exit**
  Closes the GUI and stops the firewall so Lavasoft Personal Firewall is no longer protecting your system.

**Note:**

- The system tray icon is not visible while Lavasoft Personal Firewall runs in a background mode.
Startup Mode
Lavasoft Personal Firewall allows you to control its behavior during system startup. To select one of the three startup modes, click the Options button on the Toolbar. The following modes are available under the Startup section:

Normal
The default mode. Loads automatically at boot-up and displays its icon in the system tray.

Background
If selected, Lavasoft Personal Firewall will run in invisible mode, without displaying its system tray icon or any of its dialog windows. Background mode is provided for two reasons: to save system resources and for a parent or system administrator to block unwanted traffic or content in a way that’s completely hidden from the user.

For details on background mode, see Running in Background Mode.

Disable
If selected, Lavasoft Personal Firewall will not run automatically at startup. Your system will not be protected by its firewall.
Closing and Stopping the Firewall
By default, when you minimize the Main Lavasoft Personal Firewall Window, it is minimized to the system tray icon and no task is displayed for Lavasoft Personal Firewall in the taskbar. You can alter this behavior by clicking the Options button on the Toolbar and clearing the Minimize to system tray check box in the dialog window.

Lavasoft Personal Firewall allows controlling the Main Window behavior on its closing as well. By default, when you click the close button in the right upper corner, you do not actually shut down the firewall. The Main Window is minimized and the firewall icon remains in the system tray indicating that the firewall is running and protecting your system. Clearing the Minimize main window on close check box in the Options dialog lets you tell Lavasoft Personal Firewall to stop the firewall and shutdown the service when you close the Main Window so Lavasoft Personal Firewall stops protecting your system.

You can also completely stop the firewall by selecting the Exit command on the File menu of the Main Window or by right-clicking the system tray icon and selecting the same command.
Setting the Firewall Policy

One of the most useful and important features of Lavasoft Personal Firewall is the firewall policy. A policy is the basic behavior Lavasoft Personal Firewall uses in controlling your computer's access to and by the Internet or any other network it may be connected to. The Block most policy, for example, gives Lavasoft Personal Firewall a very strict attitude but the Allow most policy makes Lavasoft Personal Firewall very trusting.

Lavasoft Personal Firewall policies

Lavasoft Personal Firewall can function according to the following policies:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚫</td>
<td>Block all</td>
<td>All network connections are allowed.</td>
</tr>
<tr>
<td>🚫</td>
<td>Block most</td>
<td>All network connections are blocked except those that are explicitly blocked by global or application rules.</td>
</tr>
<tr>
<td>🤔</td>
<td>Rules wizard</td>
<td>Helps you determine how an application will interact with the network the first time each application is run.</td>
</tr>
<tr>
<td>✅</td>
<td>Allow most</td>
<td>All network connections are allowed except those that are explicitly blocked by global or application rules.</td>
</tr>
<tr>
<td>🔄</td>
<td>Disable</td>
<td>All network connections are allowed.</td>
</tr>
</tbody>
</table>

The icon shown for each mode is displayed in the system tray as the Lavasoft Personal Firewall icon. You can tell at a glance what mode the firewall is in by looking at its system tray icon.

Changing the firewall policy

To change the current firewall policy:

1. Click the Options button on the toolbar.
2. Select the Policy tab.
3. Select the appropriate icon and click OK.

Tip:

- You can also change the firewall policy using the system tray icon’s shortcut menu. Right-click the icon, select Policy, and select the desired policy from the menu.
Running in Rules Wizard Mode

When Lavasoft Personal Firewall is first installed, the default policy is Rules Wizard. According to this policy, displays a prompt each time a new application or process (for which no rules are specified) requests network access or when an application requests a connection that is not covered by its rules. Thus lets you decide whether an application should be allowed a network connection to a specific address and port.

Lavasoft Personal Firewall also lets you specify network parameters for each type of application. Instead of having to create a new and often complex rule each time a new application is run, enables you to simply select a preset rule based on a well-known applications. The firewall even recommends the best selection for you, unless you are certain of a better choice, so you simply have to okay’s recommendation.

Create rule for OUTLOOK.EXE

Microsoft Office Outlook
Application is requesting an outbound connection

- Remote Service: DCOM
- Remote Address: 192.168.5.249

Lavasoft Personal Firewall should:
- Allow all activities for this application
- Block all activities for this application
- Create rules using preset

Select the required application from the drop-down list and click OK to make the firewall control the application according to the specific rules. You can also create your own rule for this application by selecting Custom from the drop-down list and specifying the rule settings.

This application will be included in the Partially allowed applications list.

Note:
- In the case that some application requests a connection to the server that has several IP addresses, Lavasoft Personal Firewall automatically detects all server addresses and configures the corresponding rules for all the server IP addresses according to the action you specify.
Setting the Firewall Policy

Allow Once
For applications that you are doubtful of but want to see what they do with network access. The connection will be allowed this one time. No rule is created for the application and the next time this application tries to establish a network connection, this same dialog window will appear.

Block Once
For applications that you do not trust but do not want to block totally. The connection will be blocked this one time. No rule is created and the next attempt by this application to establish a network connection results in this same dialog window.

Note:
- Rules Wizard is not supported when Lavasoft Personal Firewall is run in background mode as background mode does not include interaction with the user.
- For details on creating the application rules, see Managing Applications Network Access.
Running in Background Mode
When in background startup mode, Lavasoft Personal Firewall runs invisibly, without displaying its system tray icon or any of its dialog windows. This makes the firewall completely invisible to users thus allowing parents and system administrators to block unwanted traffic or content in a way that’s completely hidden from the user.

Another reason to use background mode is if you need to save system resources.

To have Lavasoft Personal Firewall run in background mode, click the Options button on the Toolbar and select Background under Startup.

Specifying the background/Entertainment mode policy
Because Rules Wizard policy is not supported when runs in background mode (as background mode does not include interaction with the user), you need to specify what firewall policy is applied when starts in background mode. To specify the policy that is applied in background mode:

1. Click Options on the Toolbar and select the Policy tab.
2. Select Rules Wizard.
3. Click Advanced.
4. Select the desired policy from the drop-down list in the dialog box.
5. Click OK.
Running in Entertainment Mode

When playing games or watching movies you probably want to avoid product prompts and alerts from distracting your attention or capturing focus, yet still want to be protected, especially when playing online.

Lavasoft Personal Firewall provides a specially designed Entertainment mode where protection is active without bothering users with numerous product prompts and alerts. Once the full screen application (a game, media player; etc.) is started, detects this event and suggests entering Entertainment mode, so the application runs using the background/Entertainment mode policy that is specified in Options > Policy > Advanced dialog, in which case no alerts and messages are displayed with the full screen application and updates are not checked.

If you want a particular application to always or never use Entertainment mode, select the Remember for this application check box before responding to the dialog box. You can also enable or disable Entertainment mode for specific applications in the Options > Application list using the commands on the application’s shortcut menu. Select Entertainment Mode > Enable Entertainment Mode or Disable Entertainment Mode for Lavasoft Personal Firewall to automatically change its policy when the application enters full screen mode.

To configure specific Entertainment mode settings, click Advanced. The displayed window lets you set the rules that will be used by Lavasoft Personal Firewall whenever you enter Entertainment mode, and lets you define whether advanced protection techniques such as Component Control, Anti-Leak Control and real-time spyware protection should be enabled while Lavasoft Personal Firewall runs in Entertainment mode.

Note:

- When operating in background mode, Lavasoft Personal Firewall does not enter Entertainment mode.
- When an application - with no network access rules already set - enters Entertainment mode, it is put in the Trusted applications group.
Running in Self Protection Mode
As anti-malware tools have grown stronger, hackers now try to switch them off using rootkits and other advanced tools before proceeding with their own unauthorized actions. To withstand this threat, Lavasoft Personal Firewall features so called Self-protection mode. With self-protection turned on, Lavasoft Personal Firewall protects itself against termination caused by viruses, Trojans or spyware. Even attempts to simulate user keystrokes that would otherwise lead to firewall shutdown are detected and blocked. Lavasoft Personal Firewall also constantly monitors its own components on the hard drive, registry entries, memory status, running services, and so on, and disallows any changes by malicious applications.

By default, self-protection is enabled. To disable it, click the Self-Protection button on the toolbar.

Note:
- Disabling self-protection may severely impact overall system security. Though disabling is required for the installation of plug-ins and other advanced functions, it should be re-enabled as soon as the changes have been made.
Managing Applications Network Access

One of the main principles of Lavasoft Personal Firewall’s operation is granting network access to processes and applications according to specified application rules. This allows for flexible network access setup and insures that no process can get unauthorized network access that is not covered by a rule.

Lavasoft Personal Firewall generates a list of installed applications and sets the rules for them automatically but provides an opportunity to manage the application list and rules for applications manually as well. See the appropriate sections for details.
Managing List of Applications

During the initial firewall configuration all installed applications are detected and rules for the applications are created according to built-in presets. To view a list of the detected applications, click the Options button on the toolbar and select the Application tab.

All applications as far as is concerned, are arranged in three groups:

**Blocked applications**
All network activity of applications of this group is blocked. It is recommended that you add any applications that do not need Internet access, such as text editors, calculators, etc. to this group.

**Partially allowed applications**
allows network access for these applications based on rules that were set by you manually and/or the rules presets. Only closely specified network activity is allowed for these applications. automatically detects installed applications and configures rules presets when you set the firewall configuration during installation and it is recommended that you put most applications that were not initially detected by the firewall in this group.

**Allowed applications**
All network activity of applications in this group is allowed. It is not recommended that you include an application in this group unless you trust it absolutely.

You can change the status of an application or process by simply dragging and dropping it into a different group.

You can also manage the application list by manually adding applications and removing them. To add an application, click the Add button. You will be prompted to browse to the application’s executable and, after adding the file, the Rules dialog window will be displayed so you can specify the rules for the new application. After specifying the rules and clicking OK you will be able to see the added application in the Partially allowed applications group. For more information on creating and editing application rules, see Managing Rules for Applications. To remove an application from the list, click the Remove button.

**Note:**
- You can also add an application to a list directly by dragging its icon from Windows Explorer or from your desktop into the Options > Application dialog.
- If you are using the default Rules Wizard policy, there is no need to add your applications to the list manually; will suggest rules for each application the first time an app requests network access.
Managing Rules for Applications
To list the existing rules for an application, click Options on the toolbar, select the Application tab, select the application, and click Modify Rules (or Create Rules to create rules for Blocked or Allowed applications) on the Edit menu. The Rules dialog will be displayed allowing you to manage the existing rules for the selected application and add new rules.

Adding a new rule
To create a new rule, click New in the Rules window. In the rule editor, specify the following rule parameters:

Event the rule will handle
The following criteria are available:

- Where the specified protocol is - lets you specify a protocol to be allowed or blocked.
- Where the specified direction is - either outbound or inbound.
- Where the specified remote host is - a specific IP address or DNS name.
- Where the specified remote port is - a particular port on the other computer that will be used.
- Where the specified local port is - the port on your computer that will be used.
- Where the specified time interval is - the active period of time for the request to come.
- Where local port is equal to remote port - both computers use the same port number.

Select the criteria of the event and define all the settings in the Rule Description field by clicking the underlined links.

Note:
- Local and remote port settings are available only if the protocol is defined.
- For information on using macro addresses to specify local or remote host, see Using Macro Addresses.

Actions the rule will respond with
The following actions are available:

- Allow it - Allows the connection.
- Block it - Blocks the connection (the source is not notified so it appears that the packet never reached your computer).
- Report it - Displays a visual alert when a rule is triggered.
- Run application - Runs the application with the specified command line parameters when the rule is triggered.
- Do not log this activity - disables activity logging for this rule. If selected, no data will be written to log on this rule triggering.
- Stateful Inspection - Turns on “stateful inspection” for this application (after an application connects to a remote server, all incoming data from that server to the port opened by the application will be allowed or blocked according to the specified setting).
- Ignore Component Control - Forces Lavasoft Personal Firewall to ignore Component Control during this communication.

Select the actions - the corresponding messages will be displayed in the Rule Description field. If you want a specific application to run or a command to be executed on this event, select the corresponding check box and define the application or command by clicking the underlined link in the Rule Description field.
Managing Applications Network Access

LAVASOFT PERSONAL FIREWALL

Make sure there are no undefined parameters in the Rule Description field. Lavasoft Personal Firewall will generate the descriptive Rule name automatically basing on the specified parameters.

Click OK to save the rule. The rule will be displayed in the list. The selected rule transcript is shown at the bottom of the window.

Adding rules according to presets
Lavasoft Personal Firewall lets you assign a predefined set of rules to an application. For example, if you use some an uncommon browser that was not detected by the firewall during installation, you need not create all the rules manually. Just click the Preset button in that program's Rules dialog and select Browser from the drop-down menu. All the necessary rules for this kind of application will be added automatically.

Modifying an existing rule
To modify an existing rule, highlight it in the list and click Modify. Perform any changes in the rule editor described in the rule creation section above and click OK to save the changes.

The selected rules are active (turned on) and processed by the firewall. Clear the check box next to the rule name to turn it off if you do not want Lavasoft Personal Firewall to process the rule but you don't want to delete it. You can turn the rule on any time later by selecting its check box.

Rules are applied in the top-down order (higher on the list first) but note that Lavasoft Personal Firewall uses the first rule having several criteria that match the application’s type of communication activity and ignores all subsequent ones. To change a rule's priority, highlight the rule in the list and use the Move Up/Down buttons.

You can also copy the highlighted rule within an application and remove rules using the corresponding buttons. However, you cannot copy a rule from one application to another.

Tips:
• Use the rule transcript at the bottom of the dialog to quickly change one of its parameters.
• Rules automatically created by Lavasoft Personal Firewall are marked blue in the list.
• It is prudent to save the present configuration before making changes to it.
Using Macro Addresses

Lavasoft Personal Firewall allows you to specify macro addresses in rule descriptions to facilitate the creation of rules. Instead of having to type IP addresses manually while creating rules for your Intranet communications or some Windows-based services (for example, DNS), you can use suggested macro definitions, to designate local networks as LOCAL_NETWORK, all DNS servers as DNS_SERVERS, etc.

Lavasoft Personal Firewall automatically recognizes current macro values so you do not need to change host and subnet addresses whenever network adapter settings are changed. For example, a mobile user’s protection will always be active since the rules on his laptop work regardless of what network he is connected to.

When you specify a local or remote address, you can select one of the following macros:

**DNS_SERVERS**
Specifies addresses of all DNS servers in your network.

**LOCAL_NETWORK**
Specifies addresses of all your local networks and addresses from the broadcast ranges available on your computer.

**WINS_SERVERS**
Specifies addresses of all WINS servers on your network.

**GATEWAYS**
Specifies addresses of all gateway servers for your network.

**MY_COMPUTER**
Specifies all IP addresses your computer has in different networks, including loopback addresses.

**ALL_COMPUTER_ADDRESSES**
Specifies all IP addresses your computer has in different networks, including broadcast and multicast addresses.

**BROADCAST_ADDRESSES**
Specifies addresses within broadcast ranges available to your computer. A broadcast address is an IP address that allows information to be sent simultaneously to all machines on a given subnet.

**MULTICAST_ADDRESSES**
Specifies addresses in multicast ranges. A multicast address is a single address that refers to multiple network devices. “Multicast address” is synonymous with “group address”.

---

Managing Applications Network Access

LAVASOFT PERSONAL FIREWALL

©2007 Lavasoft AB
Protecting from Malicious Process Activity

Some malicious applications can be activated as parts of legitimate programs and perform their activity on behalf of a trusted application. For example, some Trojan horses can be injected into a computer system as a module of a legitimate application (for example, your browser) and thus gain the privileges needed to connect to the person who configured the Trojan. Others can start processes in hidden mode or hijack trusted process memory to pretend to be an application you do not consider as harmful. By employing technologies of Component Control and Anti-Leak does not allow such program activity and thus fully protects you from Trojans, spyware and other dangers. See the corresponding sections for details.
Protecting from Malicious Process Activity

Controlling Application Components
Applications typically have dozens of modules, any of which can easily be substituted by virus or Trojan makers to execute a malicious code on your computer. does not just monitor applications but also each component of each application. If a component of an application has been changed and the application is about to establish a connection, will inform you of the changed component and ask whether this connection should be allowed. The technology responsible for that is called Component Control and its purpose is to make sure no fake and malicious components get network access.

Changing Component Control level
You can set up the desired Component Control level. Click Options on the toolbar, select the Application tab, and click the Components button. The following levels are available in the Component Control Settings window:

- **Maximum** - will monitor all components that are being registered as part of a legitimate application. It is recommended that you use this option only when you suspect an unknown malware to exist in your system because this option may seriously impact on your system performance.
- **Normal** - will monitor all new components as they are being registered to be a part of an application yet are not located in the application folder and all updated components and remember the legitimate ones in its database. This option is suitable for most cases and provides a balance between security and performance.
- **Low** - the same as Normal but in this case will not warn about every changed or added application component, but will warn only about executable files. It is recommended to use this option instead of completely disabling Component Control to keep the minimally necessary security level.
- **Disabled** - turns Component Control off. This option is only recommended when you experience significantly reduced performance, crashes, or other errors that lead to system instability. Turning Component Control off severely reduces your system’s security level as no longer monitors each application component.

Changing levels affects all applications and their components. It is not possible to change the level for specific applications.

*Note:* It is not recommended to use the Maximum level unless you are sure your system is being threatened by a virus, Trojan or other malicious program.

Managing shared components
You can specify the components that are to be used by more than one application. Lavasoft Personal Firewall will not warn you when a shared component is requested by an application to which it is not registered. By default, all Windows system components are added to this list because they are used by most Windows applications. You can, however, modify the list to match your specific needs.

To modify the shared components list, click Options on the Toolbar, select the Application tab, and click the Components button. Click Edit list under Shared components to display the shared components list. Add or remove specific components using the corresponding buttons.

*Note:* After you install a service pack or other software upgrade that changes a large number of files in your system it is recommended that you rebuild the shared components database so Lavasoft Personal Firewall is aware of the changes and any newly installed system components. To rebuild the database, click Rebuild database in the Shared Components dialog box.
Managing application components
Lavasoft Personal Firewall lets you manage the components it monitors for each application. All registered application components are considered legitimate and no warnings are displayed when an application requesting network access uses one of its registered components unless the component was changed.

To manage the components for a specific application, click Options on the toolbar, select the Application tab, select the application on the list, and click Edit > Modify Rules (Create Rules for allowed or blocked applications). Then click the Components button to display the components list. Add or remove specific components using the corresponding buttons.

Tip:
- In a Rules Wizard prompt for the changed component, shared components are marked red and components of a specific application are marked green.
Controlling Penetration Techniques

There are several advanced penetration schemes that allow malicious software to bypass the security perimeter of a PC. Lavasoft Personal Firewall provides proactive security functionality called Anti-Leak Control that blocks all currently-known penetration techniques that are often used by malicious programs to bypass firewall software (for details, see Understanding Penetration Techniques). This prevents sensitive data leakage from individual PCs, gives more control over what’s happening on a PC, and alerts you to spyware programs that use sophisticated techniques to hide themselves. However, some of these techniques can be used by legitimate applications in their regular activity, so it is necessary to be able to flexibly control them as simply blocking the activity can affect system stability and interrupt user work.

To enable Anti-Leak Control, click Options on the toolbar, select the Application tab, click the Anti-Leak button, and select the Enable Anti-Leak Control check box. The available settings allow you to configure which actions all applications in your system are allowed to perform. All actions are divided into dangerous that are critical and most likely will result in system instability and data leaks; and suspicious that sometimes can be used by legitimate applications for their common activity.

Select an action in the list and the right part of the window will show you the element’s description and settings. The default setting for each action depends on the security level you chose during installation. To allow or block a particular action globally for the system, select one of these available options:

- **Prompt.** will prompt you each time an application tries to perform the selected activity.
- **Allow.** The selected activity will always be allowed for all applications on your system.
- **Block.** The selected activity will always be blocked for all applications on your system.

Besides these options, you can also have show a visual notification each time an action is allowed or blocked for the application, by selecting the Report check box.

Some applications use the technology of component injection (Windows hooks) for their common activity (Nvidia drivers, for example). If you use such applications and want to allow them to inject components from the shared components list into another process’s memory, select the Allow injection of shared components check box. This setting has a higher priority than the Prompt/Block settings for Windows hooks.

If you want to have full control over all system activity of applications installed on your computer, clear the Allow all listed actions for network-enabled applications check box, otherwise it has a higher priority than the Prompt/Block settings for all listed techniques.

To individually set rules for suspicious actions from a particular application (for example, to allow a specific application to modify the memory of other processes), click the Exclusions tab. Click Add and browse to the application’s executable file. After clicking Open, you will see the application in the list and will be able to specify its individual anti-leak settings. To change the setting for the selected action, click the link in the Action column next to the action name. The available actions are the same as for the global system settings described above. Besides, you can set to inherit global setting for the action, specifying the Use Global setting.

Click OK to save your settings.

Note:

- Any actions that are over other instances of the same process are allowed. For example, Internet Explorer can control other Internet Explorer windows.
- If you completely trust an application and want to allow it to perform all the listed actions, right-click the application in the list on the Application tab and select Ignore Anti-Leak Control. The application will be added to the Anti-Leak exclusions list with all actions set to Allow.
Understanding Penetration Techniques

Lavasoft Personal Firewall allows you to control the following actions:

Components injection
Windows operating systems—by design—enable installing system interceptors (hooks) through which foreign code can be injected into processes. Normally, this technique is used to perform common, legitimate actions, such as switching the keyboard layout or launching a PDF file within the web browser window. However, it can also be used by malicious programs to embed harmful code and thus hijack the host application. An example of a leak test that uses such a technique to stage a simulated attack is the PC Audit program (http://www.pcinternetpatrol.com/).

Lavasoft Personal Firewall controls the installation of a hook interceptor in a process's address space. This is implemented via the interception of functions that are typically used by malicious processes (Trojans, spyware, viruses, worms etc.) to implant their code into legitimate processes, such as Internet Explorer or Firefox. The behavior of a DLL file invoking such functions is considered suspicious and triggers a legitimacy verification.

Control over another application
DDE technology is used to control applications. Browsers are commonly DDE servers, so can be used by malicious programs to transfer private information onto a network. One example of this technique is the Surfer leak test (http://www.firewallleak tester.com/leak test15.htm). ZABypass is another example of a leak test that uses this method.

With Lavasoft Personal Firewall, every attempt to use DDE intercommunication is monitored with no exclusion, whether the process is open or not. The DDE inter-process communication control enables to govern the methods used by applications to gain command over legitimate processes. It prevents malware from hijacking a legitimate program and checks whether such DDE-level interactivity is allowed to be performed on network-enabled applications. In case such an attempt is detected, it triggers a legitimacy verification prompt.

Application window control
Windows allows applications to exchange window messages between processes. Malicious processes can gain control over other network-enabled applications by sending them window messages and imitating user input from the keyboard and/or mouse clicks. An example of using this technique is the Breakout leak test (http://www.firewallleak tester.com/leak test16.htm).

The crucial point here is program interactivity through the SendMessage, PostMessage API, and so on. This technique is used for legitimate inter-process interactivity, but can very easily be used for nefarious purposes by malicious individuals.

Lavasoft Personal Firewall controls such attempts.

Active Desktop modification
Creating an HTML page pointing to a certain website and setting it as a Windows Active Desktop, malicious processes can transfer private data on behalf of Windows Explorer. When the Active Desktop is turned on, it is permitted to go to the website address contained in the HTML page, acting on behalf of the system and thus bypassing firewall’s sensors. An example of using this technique is demonstrated by the Breakout leak test (http://www.firewallleak tester.com/leak test16.htm).

Lavasoft Personal Firewall controls such attempts to steal data by bamboozling the firewall.
DNS query submission
The DNS Client service contains a vulnerability called DNS tunneling. Malicious code can transfer and receive any information using correct DNS packets to a correctly configured operating DNS server. An example of using this technique is the DNSTester leak test (http://www.klake.org/~jt/dnshell/).

Lavasoft Personal Firewall performs double verification of any access to a DNS Client service, thereby providing a more secure system. This controls access to a DNS API even with the DNS Client service on, and thus benefits users who, out of compatibility concerns, cannot disable this service themselves. This functionality allows the assignment of permissions to a specific process to use the DNS Client service.

Application launch with URL
Malicious processes can launch the default web browser with a pre-configured web address in a hidden window, making the firewall believe a legitimate action is taking place. Firewalls that explicitly trust an application without looking beyond—to who actually launched it in the first place and what additional connection parameters are supplied—are unable to challenge the technique, and thereby allow confidential data to be transmitted from the computer. The examples of using this technique are Tooleaky and Ghost leak tests (http://www.firewallleaktester.com/leaktest2.htm, http://www.firewallleaktester.com/leaktest13.htm).

Lavasoft Personal Firewall watches every program started on a computer and controls who has the permission to start each program with the target URL and will prompt the user as to whether such activity should be permitted for a particular program.

Application launch with command line parameters
Several firewalls are exposed to the vulnerability of predatory code launching the default web browser with command-line parameters. These firewalls allow themselves to be circumvented because they are made to believe a legitimate application is performing legitimate actions. However, one or more of those command-line parameters can be private or critical data that gets sent along to the host name. An example of this technique is the Wallbreaker leak test (http://www.firewallleaktester.com/leaktest11.htm).

Lavasoft Personal Firewall has a restricted list of processes that are allowed to start the default browser with command line parameters, which protects your browser against tampering. Beyond browsers, command-line launch control applies to all network-enabled applications, which are present in the configuration.

Critical registry entry modification
The registry is a universal repository of system settings and program configurations. Modifying its content can lead to application errors or even system failure. Malicious processes use this technique to make small modifications to the registry elements, enabling an unverified process to unrestrictedly access the network, in spite of the presence of a firewall, by adding its components to the applications, for example, Windows Explorer, and acting on their behalf. An example of using this technique is the Jumper leak test (http://www.firewallleaktester.com/leaktest17.htm).

These attempts are controlled by Lavasoft Personal Firewall. This proactive capability lets you allow or prevent the embedding of objects into a certain area of the registry.
OLE application control
A relatively new technique has surfaced that controls application activity through OLE (Object Linking and Embedding)—a Windows mechanism, which allows one program to manage the behavior of another program on the computer. It uses the technique of OLE intercommunication to exchange data and commands between applications, for example, to manage the activity of Internet Explorer so it can send user-specific data to a remote location. An example of using this technique is the PCFlank leak test (http://www.pcfllank.com/PCFlankleak test.exe).

Lavasoft Personal Firewall detects an OLE communication and asks the user if it is normal for that application to control other applications’ activity.

Process memory modification
Several Trojan horses and viruses use sophisticated techniques that let them alter the code of trusted applications running in memory and thereby bypass the system security perimeter in order to perform their malicious activities. This is known as code injection or copycat vulnerability. Examples of using this technique are the Thermite and Copycat leak tests (http://www.firewallleak tester.com/leak test8.htm, http://www.firewallleak tester.com/leak test9.htm).

Lavasoft Personal Firewall enables you to control the functions that can be used to write malicious code into a trusted application’s address space and so prevent a rogue process from injecting their code into those processes. The entire memory space used by any active application on a computer is monitored by (not just that of a network-enabled application). If malware tries to modify a legitimate application’s memory, detects it and displays a pop-up alert. The system works proactively: it allows you to permit or deny the modification of memory of other processes at the application level. For example, Visual Studio 2005 would be able to modify memory, while the “copycat.exe” leak test would be disallowed from doing so. This feature protects against even unknown malware not yet detected by antivirus and anti-spyware vendors that exploits this vulnerability.

Low-level network access
Some network drivers allow direct access to the network adapter, which bypasses the standard TCP stack. These drivers can be used by sniffers and other malicious programs to get low-level network access. They pose an additional risk for the system as traffic passing through them cannot be screened by a firewall. The example of using this technique is MBtest leak test (http://www.firewallleak tester.com/leak test10.htm).

Lavasoft Personal Firewall allows the control of applications that request non-standard network access. This feature strengthens overall network security level by preventing outbound data leakage. The user is able to control an application’s attempts to open a network-enabled driver; so without the user’s authorization, an application is not able to send even the ARP or IPX data.
Managing Global System Network Activity

Besides controlling network access on an application level, Lavasoft Personal Firewall enables advanced users to control all system traffic on all levels as well.

With Lavasoft Personal Firewall, you have the following opportunities:

- Define rules for all processes running on the system - called global rules
- Control the system’s ICMP traffic
- Run the firewall in a stealth mode
- Control network access through rawsockets

See each corresponding section for details.

Note:

- These settings are for advanced users only. If changed incorrectly, it could result in your firewall not working as expected. In most cases, you do not need to modify these rules or add yours.
Managing Global Rules

Global firewall rules are applied to all processes and applications on your computer that request network access. You can, for example, block all traffic that uses a specific protocol or all traffic from a particular remote host by creating the appropriate rules. Provides several predefined global rules designed for optimal system functioning. To view the global rules list, click Options on the toolbar, select the System tab and click Rules under Global rules and rawsocket access.

Adding a new rule

To add a new rule, click Add in the Global Rules window. In the rule editor you should specify the following rule parameters:

Event the rule will handle

The following criteria are available:

- Where the specified protocol is - lets you specify a protocol to be allowed or blocked (with the ability to specify the protocol type for IP protocol).
- Where the specified direction is - either outbound or inbound (with the ability to specify the packet type for outgoing traffic).
- Where the specified remote host is - a specific IP address or DNS name.
- Where the specified remote port is - a particular port on the other computer that will be used.
- Where the specified local host is - your computer IP address or DNS name.
- Where the specified local port is - the port on your computer that will be used.
- Where the specified time interval is - the active period of time for the request to come.
- Where local port is equal to remote port - both computers use the same port number.

Select the criteria of the event and define all the settings in the Rule Description field by clicking the underlined links.

Note:

- Local and remote port settings are available only if the protocol is TCP or UDP.
- For information on using macro addresses to specify local or remote host, see Using Macro Addresses.

Actions the rule will respond with

The following actions are available:

- Allow it - Allows the connection.
- Block it - Blocks the connection (the source is not notified so it appears the packet never reached you computer).
- Report it - Displays a visual alert when a rule is triggered.
- Run application - Runs the application with the specified command line parameters when a rule is triggered.
- Do not log this activity - disables activity logging for this rule. If selected, no data will be written to log on this rule triggering.
- Mark rule as High Priority - Sets the rule to prevail over the application rules which take precedence by default.
- Stateful Inspection - Turns on “stateful inspection” for this application (after an application connects to a remote server, all incoming data from that server to the port opened by the application will be allowed or blocked according to the specified setting).
Managing Global System Network Activity

- Ignore Component Control - Forces Lavasoft Personal Firewall to ignore Component Control during a communication.

Select the actions - the corresponding messages will be displayed in the Rule Description field. If you want an application to run or a command to be executed on this event, select the corresponding check box and define the application or command by clicking the underlined link in the Rule Description field.

Make sure there are no undefined parameters in the Rule Description field. Lavasoft Personal Firewall will generate a descriptive Rule name automatically based on the specified parameters.

Click OK to save the rule. The rule will be displayed in the list.

Modifying an existing rule
To modify an existing rule, highlight it in the list and click Edit. Perform any changes using the rule editor described in the rule creation section above and click OK to save the changes.

Selected rules are active (turned on) and processed by the firewall. Clear the check box next to the rule name to turn it off if you do not want Lavasoft Personal Firewall to process the rule but you don’t want to delete it. You can turn the rule on any time later by selecting its check box.

Rules are applied in top-down order (highest on the list first) but note that Lavasoft Personal Firewall uses the first rule that has several criteria that match the type of communication activity and ignores all subsequent ones. To change a rule’s priority, highlight the rule in the list and use the Move Up/Down buttons.

You can also copy a highlighted rule or remove a rule by using the corresponding buttons. It is not recommended to remove any built-in global rules.

Tip:
- It is prudent to save the present configuration before making changes to it.
Controlling ICMP Protocol Activity

Internet Control Message Protocol (ICMP) is used to send error/control messages between computers connected on a network. It allows you to specify the types and directions of the ICMP messages allowed.

To specify the ICMP settings, click Options on the Toolbar; select the System tab and click Settings under ICMP. In the ICMP Settings dialog, the main ICMP message types are listed; you can allow incoming or outgoing messages by selecting the corresponding check boxes by its side. If a check box is cleared, the connection is blocked.

Use the Default button to reset all the ICMP settings to the default ones.

Note:
- It is recommended that you do not change the ICMP settings unless you are certain that you are making the right changes.
- The different types of ICMP messages are described in Appendix B: Types of ICMP Messages of the user’s guide.
Running in Stealth Mode
Stealth mode allows you to define whether your computer will respond to port scans or to silently block them, making itself invisible to hackers.

Normally, when your computer receives a connection request to a port not used for any incoming or outgoing connections, it lets the other computer know that this port is not used by sending a “port unreachable” notification. In stealth mode, your computer will not respond, making it seem like it is not turned on or not connected to the Internet. In this case, packets sent to the unused port are simply ignored by the firewall without notifying the source via any ICMP or TCP message.

To set the firewall to stealth mode, click Options on the Toolbar, select the System tab and then Stealth under Firewall mode.

Note:
• It is recommended that you keep in stealth mode unless you have some reason not to.
Controlling Rawsockets Access

Some applications can access a network directly through low-level socket calls, also known as rawsockets. These calls cannot be governed by ordinary protocol and application rules and thus can serve as a backdoor for a rogue application or as a way to access a network without limitation or regulations.

To improve your system’s protection, Lavasoft Personal Firewall enables you to control rawsocket access. You can define which applications are allowed to make rawsocket calls and which are not. To manage the list of applications that are allowed to use rawsockets, click Options on the toolbar; select the System tab and click Rawsockets under Global rules and rawsocket access. Click Add and select the application you want to grant rawsocket access to.

If you want Lavasoft Personal Firewall to ask you each time an application that is not on the allowed list attempts to access rawsockets, select the corresponding check box.

Note:
- Once an application is added to this list, it is granted unrestricted network access.
Configuring Local Network Settings

A fundamental difference between a local area network (LAN) and the Internet is the level of trust you can have in each. A LAN used in the home or an office is generally comprised of “friendly” computers, computers belonging to or operated by other family members or fellow workers.

Lavasoft Personal Firewall allows you to detect the networks your computer belongs to and define the specific access level for each network.
Detecting a Local Area Network

Normally, LAN settings of your computer should be detected and configured during the installation of . But if you chose manual configuration during the installation and/or removed all detected networks, then you will have to detect your LAN newly in order to normally communicate with other computers.

To view the list of networks to which your computer belongs, click Options on the Toolbar, select the System tab and click Settings under LAN settings.

Detecting a LAN automatically

In the LAN Settings dialog, click Detect and will automatically detect the networks your computer belongs to and create a list of their IP addresses, specifying the default level of access for each detected network. You can then fine-tune the appropriate access levels for each network.

For to automatically detect a new network so you will not have to add it manually, select the Auto-detect new network settings check box and click OK to save this setting.

Adding a network address manually

If you prefer to add another network or remote host to the list and to configure a specific access level for it or if for some reason did not detect your networks automatically, you can do this manually. In the LAN Settings dialog, click Add and in the Network Address dialog specify the format you wish to use to enter its address. The following options are available:

- Domain name. For example, http://www.lavasoft.com. An active Internet connection is required in this case because the IP address needs to be looked up directly over the Internet. The IP address is saved along with the domain name you enter and it is this IP address that is used by .
- IP address. For example, 216.12.219.12.
- IP address with subnet mask. For example, 216.12.219.1 - 216.12.219.255.

Type in the desired address in the format you selected (wildcards are allowed) and click Add. You can add several addresses in sequence this way and then click OK to add them to the list in the LAN Settings dialog. Configure the appropriate access levels for each network and click OK to save the settings.

Removing an address from the list

You can remove a selected address or network from the list by clicking the Remove button. Actually removing the address from the list is similar to specifying the Limited Access to LAN level for that address (i.e. clearing both the NetBIOS and Trusted check boxes).

Note:
- For details on configuring LAN access levels, see Specifying LAN Access Levels.
Specifying LAN Access Levels

All computers on a LAN can be assigned one of three levels of access regarding your computer:

- NetBIOS access. Only File and Printer Sharing between the LAN and your computer is allowed. To set this level, select the NetBIOS check box for this address.
- Trusted. All connections to and from the network are allowed. To set this level, select the Trusted check box for this address.
- Limited Access to LAN. NetBIOS communications are blocked, all other communications are handled by application and global rules. To set this level, clear both the NetBIOS and Trusted check boxes for this address.

It is very important to remember that a host on a Trusted network is given the highest priority possible. Even restricted applications can communicate with a host. It is recommended to set only absolutely trusted computers as Trusted. If you just need File and Printer Sharing, use NetBIOS rather than Trusted.

If you do not want to clutter up logs with information about NetBIOS broadcast packets, you can specify to disable these data logging for each of the detected host or subnet. Select the address from the list and clear the Log NetBIOS broadcasts for selected host or subnet check box in the Information area. This will keep Log Viewer data more clear and may improve computer performance.

Note:

- NetBIOS broadcast packets are inbound or outbound UDP packets with the sender’s address belonging to the selected subnet and sent to 255.255.255.255 address from 137 or 138 port to the same port. Such packets, for example, are used by the client computers to reveal their presence in the network.
- Please note that ’s plug-ins are independent from the address access level. For example, even if you add www.lavasoft.de to Trusted network addresses, the plug-ins will still block banners, active content, etc. from this site and perform their common activity regardless of the address access level.
Protecting Firewall Settings

Lavasoft Personal Firewall enables you to protect the settings you specify from being altered without your authority. Being secured by a password, firewall settings cannot be changed by another person. You can, for example, block access to objectionable sites for your children and know that your settings cannot be tampered with.

Setting the password
To set the password, click Options on the Toolbar and select Enable under Password protection. Specify the password, click OK and confirm your password in the displayed window. Click OK once again to save the password, and it will start protecting your settings after you close the Options dialog. After that, every time somebody tries to gain access to the firewall settings or create a new configuration, he will be prompted for this password.

Changing the password
To change the password, click Options on the Toolbar, specify the password, and click Set password under Password protection. Specify and confirm the new password, then click OK. Changes will take effect after you close the Options dialog.

Disabling the password
To disable the password, click Options on the Toolbar, specify the password, and click Disable under Password protection. After you click OK, all firewall settings will be available to every person who uses the computer.

By default, your password protects your configuration settings only from being altered, but you can additionally protect the Log Viewer from being launched and its service from being stopped by selecting the corresponding check boxes. This allows you to keep the system network history from being viewed by unauthorized persons and prevents the service from unloading and disabling its protection and the restrictions you set. This is most useful for parents who want to control their children’s Internet access and employers who need to restrict the activities of their employees.

Note:
• Please remember your password. If you forget the password, you will have to reinstall.
Preventing Network Attacks

A major function of firewall protection is inbound filtering, which controls all incoming activity to block hackers and malicious programs when they try to attack your computer.

The Attack Detection plug-in detects, prevents, and reports all possible attacks on your computer from the Internet or the network your computer is connected to. It screens inbound traffic and determines its legitimacy either by comparing it against a set of known attack patterns or by performing behavior evaluation analysis. The Attack Detection plug-in can detect not only every known type of attack (such as port scanning, Denial of Service (DoS) attacks, attacks of ‘short fragments’ and ‘my address’ classes, and many others) but future exploits as well.

Setting port scanning alarm level

You can define how sensitive Lavasoft Personal Firewall should be in detecting attacks by setting the desired alarm level. The alarm level determines the number of suspicious packets detected before reports an attack is detected. To set the alarm level, right-click the plug-in in the Left Panel and select Properties. Move the slider to one of the following values:

- High. An attack alert is displayed even if a single scan of one of your ports is detected.
- Normal. An attack alert is displayed only if several ports are scanned or if a specific port is scanned that recognizes as one commonly used in attacks.
- Low. An attack alert is displayed only if a multiple attack is definitely detected.

Change the alarm level depending on the risk your computer runs or if you are suspicious, set the level to high.

You can also adjust the sensitivity to attacks, by specifying the number of suspicious packets required for an alarm at each level. To do this, click the link under the slider to set the numbers.

To receive visual and/or sound alerts about detected attacks, select the Show visual alert when attack is detected and/or the Play sound alarm when attack is detected check boxes.

Blocking attackers

After Lavasoft Personal Firewall detects an attack, it can change its behavior to automatically protect you from any future attacks from the same address. To do this, select the Block intruder for check box and all traffic from the computer attacking yours will be blocked for the number of minutes you designate. The default value is 5 minutes.

You can also set Lavasoft Personal Firewall to block the entire subnet the attacker’s address belongs to by selecting the Also block intruder subnet check box.

Protecting from Ethernet attacks

When data is sent from one computer to another over a local network, the sending machine broadcasts an ARP (IP-to-Ethernet address lookup) request to determine the MAC address based on the IP address of the target machine and waits for it to send back its MAC address. During the time between the packet broadcast and the MAC address response, data is vulnerable to tampering, hijacking, and/or redirection to an unauthorized third party.
The Attack Detection plug-in also protects your system from invasions on a local network. It detects and blocks Ethernet attacks such as IP spoofing, ARP scanning, ARP flood and others by inspecting your Ethernet and/or Wi-Fi connections. To specify the Ethernet attack prevention settings, select the Ethernet tab in the plug-in properties window. The following options are available:

- **Enable smart ARP filtering.** Prevents ARP spoofing - where a node starts sending a huge number of ARP replies with varying MAC addresses in a short time span, trying to overload the network equipment as it tries to determine which MAC address actually belongs to the node. If enabled, Lavasoft Personal Firewall only permits incoming replies from other hosts for which there was a previous outgoing request. Only the first ARP reply is accepted for each request. Smart ARP filtering also protects from ARP cache poisoning, which occurs when someone succeeds in intercepting Ethernet traffic using fake ARP replies in an effort to change the address of a network card to one that an attacker can monitor. Additionally, it prevents ARP floods - where a huge number of bogus ARP replies are sent to the target machine freezing a system.

- **Detect IP address spoofing and block IP flood.** Detects when an attacker falsifies or forges his IP address and blocks abnormal volumes of traffic which may otherwise overload a computer. This option cannot stop the network from being flooded but can protect the PC from overload.

- **Prevent gateway network adapter MAC spoofing.** Detects any attempt by an attacker to associate a gateway network adapter IP address with their own MAC address to allow them to intercept packets. Hackers can substitute legitimate MAC addresses with ones of their own and reroute legitimate traffic to a hacker-controlled machine, by sending out forged ARP responses which will detect and block. This ARP spoofing enables hackers to be able to 'sniff' (read) packets and view any data in transit, to direct traffic to non-existent hardware causing delays in data transmission or a denial of service on the affected equipment. Specialized hacker sniffing programs can also intercept traffic, including chat sessions and related private data such as password entries, names, addresses, and even encrypted files, by modifying MAC addresses at the Internet gateway.

- **Protect my IP addresses from being falsely reported as used.** Detects cases where two or more hosts share the same IP address. This can be due to an attacker attempting to gain access to network traffic or block a computer from accessing the network, but could also happen legitimately where an ISP uses multiple servers for load-sharing. If enabled, Lavasoft Personal Firewall blocks ARP replies that have the same IP (but different MAC’s) and thus protects computer from the IP address duplication consequences.

- **Block hosts enumerating other computers on LAN.** Limits the number of ARP requests enumerating IP addresses from one MAC address during a specified time interval which can imply network scanning. Some massively propagating viruses use mass host enumeration to hop from one computer to another, infecting them as they go. This technique is also used by scanners and vulnerability analyzers.

**Specifying attacks to detect**

You can designate what attacks Lavasoft Personal Firewall is to detect and block. By default, more than fifteen different types of attack or exploit are handled, but you can select not to detect certain types to lower your system resource usage or to stop too-frequent or faulty alert messages that may appear if, for example, a trusted service in your network is falsely perceived as an attack source.

To customize the attack detection list, select the Advanced tab of the plug-in properties window and click Edit list under Attacks list. Click Advanced to set some extra settings such as attack duration time and click OK in both windows to save the settings.
Paying special attention to vulnerable ports
From the security point of view TCP and UDP ports in your system are divided into several groups according to probability of an attacker to use a port to break into your system. Typically, ports assigned to vulnerable services like DCOM or RPC should be monitored with greater care because they are more likely to be an attack target.

However, you may have custom services assigned to custom ports that are also a lure for an attacker. The Attack Detection plug-in lets you set selective preferences for different ports and create a list of ports to which it will pay more attention while monitoring network traffic.

To specify a port that you consider vulnerable, select the Advanced tab of the plug-in properties and click Specify under Vulnerable ports. Vulnerable ports are divided into two groups: system ports and Trojan ports. Add ports that are used by vulnerable system services to the system ports list. Add ports that are exploited by well-known Trojan horses to the Trojan ports list. Select the tab according to the list you want to change.

To add a port, click Add and specify the following parameters: protocol, port number and weight. Weight is a decimal value that indicates that port’s importance. A greater number indicates a more vulnerable port. You may also add optional comments in the corresponding field to describe the port’s purpose or anything else you’d like noted.

Specifying trusted hosts and ports
There may be computers that you are absolutely sure are not a source of danger to your system as well as ports on your system you are sure cannot serve as an intruder’s backdoor. In other words, you consider any monitoring of these hosts and ports unnecessary and prefer to conserve system resources and performance by not monitoring them. The Attack Detection plug-in features exclusion lists to which you can add hosts and ports you don’t want to be monitored.

To add a host or port to the trusted list, click the corresponding button under Exclusions on the Advanced tab of the plug-in properties and add the desired host or port.

Note:
- To see a list of attacks the Attack Detection plug-in has blocked, select the plug-in in the Left Panel and click the Show Detailed Log button on the Information Panel. Log Viewer will display its log for the Attack Detection plug-in. For more information about the ‘s log system, see Tracking Network Activity.
Tracking Network Activity

For your convenience all network-related actions and events occurring on your computer are logged in details and can be viewed using a special application called the Log Viewer, which shows every application and connection that was allowed or blocked by , the specific activities of each plug-in, the start of every program and all changes made to policies, configuration settings and passwords.

Log Viewer allows for flexible customizing of its data display so you can view only the information you need, sort it the way you need. It lets you filter data by any parameter - port, host, application and others.

To start Log Viewer, select Log Viewer on the Tools menu in Main Window.

Note:
- Lavasoft Personal Firewall logs can also be viewed via the Microsoft Management Console (MMC) snap-in. To view the logs through MMC, open the MMC console, select Add/Remove Snap-in on the File menu, click Add and select Logs from the list. Click Add, Close and OK to add the snap-in to the console.
Log Viewer Interface

When you launch Log Viewer, its main window is displayed. From the main window you can select the log, viewing information and modify the Log Viewer settings. In general, the elements of the Log Viewer main window are similar to the elements of main window and are managed similarly.

To display Log Viewer when Lavasoft Personal Firewall is minimized to the system tray:

1. Right-click the firewall’s system tray icon.
2. Select Show Log Viewer.

The Log Viewer main window contains:

- Menu bar - The menu bar contains different commands for working with Log Viewer.
- The Toolbar - See The Toolbar section for details.
- Folder bar - Displays the name of the tree node currently selected in the Left Panel.
- Left Panel - See the Left and Information Panels section for details.
- Information Panel - See the Left and Information Panels section for details.
- Status bar - The status bar is the bottommost part of the Log Viewer main window used to display the Lavasoft Personal Firewall current state, the number of the selected record and the total number of records displayed in the Information Panel.
Left and Information Panels

To represent the collected information in a user-friendly manner, Log Viewer uses two panels. The Left Panel is similar to the Left Panel of Windows Explorer. It provides a listing of the logs and filters. Information Panel gives specific data stored in any log highlighted in the Left Panel.

As with Windows Explorer, any line that starts with a plus sign (+) can be expanded to show each of its subcategories. Any line starting with a minus sign (−) shows that the line has already been expanded. By clicking on the minus sign, all of its subcategories can be hidden to conserve screen space.

By default, Left Panel lists and the Information Panel displays the contents of the following logs:

- Alerts Tracker - Displays all the visual alerts shown to the user.
- Allowed Connections - Displays all the connections that Lavasoft Personal Firewall has allowed.
- Anti-Leak - Displays all the events of Lavasoft Personal Firewall's Anti-Leak Control.
- Blocked Connections - Displays all the connections that Lavasoft Personal Firewall has blocked.
- Component Control - Displays all the events of Lavasoft Personal Firewall's Component Control.
- Attack Detection - Displays every suspicious activity and attacks on your computer from the Internet, the ports involved and where the attacks are from. For information about the Attack Detection plug-in, see Preventing Network Attacks.
- System Log - This is a record of every program started and every change made to the firewall policies, program options and configuration settings.

For each group of logs (except the Alerts Tracker, Component Control, and System Log), several helpful filters are created by default.

Note:

- You can create your custom filters based on your own needs and add them to the groups in the Left Panel.
Creating Multiple Configurations

The exact state of Lavasoft Personal Firewall at any moment of time is represented by all of its settings, which include: application and global rules, LAN settings, plug-in exclusion lists, etc. The totality of these settings is called the configuration. The first configuration is created during installation. You can always modify any of the settings and even create different configurations for different activities. This allows for separate configurations for each computer user; configurations to prevent children from accessing unacceptable sites, from playing online games or chatting if they use their parent’s computer. This makes it easy to transfer configuration settings from one computer to another and easy to back up your configurations. Switching between configurations is very quick.

To create a new configuration, select New Configuration in the File menu. The Configuration Wizard will help you create a new configuration.

The Configuration Wizard provides two ways to configure your firewall: automatic configuration or by letting the Configuration Wizard help you. The first step lets you select whether you want to create a configuration automatically or specify each of its settings manually.

Automatic configuration
You can select an automatic configuration that conforms to the security level you’d prefer. Two levels are available: Advanced security provides the best protection against all penetration techniques that are often used by malicious software to bypass firewall software and Normal security ensures protection only against the more dangerous techniques (for details, see Protecting from Malicious Process Activity). Normal security has a reduced number of product prompts that require your response and is recommended for most cases.

Automatic configuration is much faster than custom. After you select either Advanced security or Normal security and click Next, the Rules Autocreation step is displayed, which allows you to enable rules autocreation, so that global rules and rules for well-known applications are created automatically when they first request an action (for example, network access or process memory modification). If you do not want to enable rules autocreation, select Use predefined rules for detected applications for the rule sets to be created according to our engineers’ built-in presets in order to provide optimal system performance and application security.

After clicking Next, automatically scans your system and adjusts all its settings without your supervision. It configures network settings, builds the Component Control database, and, in case you selected to use predefined rules, searches for known applications installed on your computer that might require Internet access and configures an appropriate the network access level for each of them.

Note:
- If Normal security level is selected, some of the more exotic security test programs (leaktests) will be failed.

Custom configuration
If you select Custom configuration, the Configuration Wizard will guide you through the configuration process, allowing you to fine-tune the firewall for each of your specific needs, as well as select the specific configuration settings for each of the networks to which your system is connected and for each of your installed network-enabled applications. By modifying these configuration settings you can define the precise security levels that Lavasoft Personal Firewall provides. The wizard lets you produce a fully customized configuration, but it takes considerable time and assumes you have advanced knowledge of Windows and your system.
Creating Multiple Configurations

After clicking Next, the Rules Autocreation step is displayed allowing you to enable rules autocreation, so that rules for well-known applications and global rules are created automatically when each application first requires an action (for example, network access or process memory modification). If you do not want to enable rules autocreation, select Use predefined rules for detected applications for the rule sets to be created according to our engineers’ built-in presets to provide optimal system performance and application security.

Click Next and Lavasoft Personal Firewall will automatically detect your network environment. On the Network Configuration step you will see a list of the networks to which your system is connected. To view and edit the network settings, click the Change button. You can change these settings at any time when working with Lavasoft Personal Firewall. For details see Configuring Local Network Settings.

If you selected to use predefined rules, after clicking Next, Lavasoft Personal Firewall starts searching for the known applications installed on your computer, which might require Internet access, and configures a network access level for each of them. On the Searching for Applications step you can view a list of those applications and edit each suggested security rule using the Details button. You can cancel rule configuration for a specific application by simply clearing the check box to the right of its name. Click OK to save and Next to proceed. You can change these settings at any time when working with Lavasoft Personal Firewall. For details see Managing Applications Network Access.

After clicking Next, the Component Control database is collected and the wizard automatically proceeds to the last step.

On the final step you can configure other Lavasoft Personal Firewall settings, such as firewall policy, global rules, and others by clicking the Advanced button. The Options dialog then lets you alter any Lavasoft Personal Firewall settings. By default the created configuration is called configurationN.cfg (where N is an increasing index) and is saved in the Lavasoft Personal Firewall installation folder. If you prefer to save it to another location, click Change and specify its path.

Click Finish to apply the changes and save the configuration.

You can create several configurations based on the current settings simply by giving each a different name using the Save Configuration As command on the File menu. To change to a new configuration, select Load Configuration on the File menu and select the configuration file you want or simply select the configuration name on the File menu.

A configuration can be protected from being modified or swapped by specifying a password. For details see Protecting Firewall Settings.

Note:
- When exiting Lavasoft Personal Firewall, the configuration file that is currently in use is saved so it will be automatically loaded the next time Lavasoft Personal Firewall is started.
Contacting Technical Support

If you need assistance in working with Lavasoft Personal Firewall, please visit the support page at http://www.lavasoft.com/support/supportcenter/index.php. Among available support options are the knowledge base, documentation, support forum, product-related web resources, and direct contact with support engineers.