

What's new in this version

Jetico Personal Firewall v2 offers a number of new features.

Removed features

- Windows 9x/Me system support discontinued. Please use Jetico Personal Firewall v1 for these systems.

System-related changes

- Jetico Personal Firewall v2 runs as privileged Windows service. It can protect computer before user logon.
- Native support for Windows XP Fast User Switching and Terminal Services.
- Jetico Personal Firewall supports Access Control Lists for all main functions. Administrator can configure ACL to grant access to particular firewall functions for any user or group.
- Windows XP Service Pack 2 Security Center support.

User interface changes

- Improved rule editing interface.
- New popup message. The new look for popup dialog is presented. Popup message text and rule creation options can be modified.
- Firewall variables formerly controlled by Configuration Wizard, are integrated into main application window.
- Language file support for easy localization. All translatable words and phrases are taken from single UTF-8 encoded text file.

Configuration changes

- New XML-based open configuration file format. Detailed documentation is available upon request.
- The new version maintains single protected firewall configuration for all users.
- Simplified controls for configuration.
- New hash handling scheme. Separate table for hash checking.
- Each firewall filtering layer has own root table.
- New automatic variables (per-connection) for local connections are supported.

Changes in firewall rules

- Rules support lists of parameters where possible.
- [IP rules](#) support IP address ranges.
- Low level protocol rules support filtering by MAC address.
- Application rules have events for direct and indirect access to network. Indirect access details are also available.
- New module for hash checking created.
- Application, Process attack and Hash checking rules support wildcards in file paths.

Logging subsystem changes

- Log entries can be associated with rule.
- Firewall can create rule based on log information.
- New WELF-compatible text log format. WELF is supported by many log analyzers.
- Improved log control.

Related info:

[Network packet filter](#)

[Application filter](#)

[Process attack filter](#)

Why do you need a firewall

Once you are connected to the Internet your computer becomes visible to wide wild world of public networks. Your computer could be accessed outside in the same way as servers you are accessing to.

[Crackers](#) scan the Internet looking for victims and any computer could be chosen as the next target for remote attacks over the network. Attack motivation may vary from idle curiosity or spiteful joke to ill-intentioned crime. If an attack succeeds, the victim may suffer from loss of valuable information, system damage etc.

Let's list major actions representing danger to computers connected to the Internet:

- Operating system or installed software bugs could be exploited to inject and execute unauthorized programs on your computer. Such programs are able to grab full control over your computer and remain for a long period of time (say month or more). Software vendors do release patches and updates, but only a portion of computers are kept up-to-date.

- The next attack type is [Denial of Service](#). A malicious person does not gain access to your computer, but instead makes your system virtually unusable. Repeating crashes, reboots, or sudden system slowdown may indicate that you are under attack.

- Camouflaged hazardous programs, [Trojans](#) may be embodied into email attachments, web pages or software. Trojans can steal sensitive information or just enable remote control over your system for intruders.

- Incorrect security configuration may lead to potential leaks of personal and other sensitive information. For example, cookies accepted by a web browser make possible gathering statistics on your activity.







- Finally let's mention annoying importunate information (mostly ads): spam, banners, popups.
- The things mentioned above frustrate and embarrass users.

A [Firewall](#) makes your system more secure and less visible to malicious persons. Both factors reduce the risk of being cracked. A firewall allows you to inspect and restrict all incoming and outgoing traffic using a set of rules. Thus it is up to you whether to allow or block any network connection.

Correctly configured, a firewall is capable of protecting your computer from practically any attack. It should be mentioned that a firewall running at your Internet Service Provider's host is a great advantage for your security, but some attacks can be blocked at the PC end of connection only.

Jetico Personal Firewall benefits

Jetico Personal Firewall combines a set of unique features. The main advantages are outstanding security and simplicity. The following key principles constitute the solid basis for Jetico Personal Firewall.

-  **The highest protection level** based on multi-level filtering. Jetico Personal Firewall establishes filters at multiple layers in the operating system. This allows our software to withstand all known attacks.
-  **Easy to use.** Jetico Personal Firewall has a powerful yet simple user interface. It was arranged carefully, so that all major functions become available in one touch.
-  **Fine tuned configuration.** The firewall package contains several pre-built configurations to satisfy everyone's needs.
-  **Live configuration.** Jetico Personal Firewall Configuration explorer displays effective configuration as well as rule activity indicators.
-  **Open architecture.** The entire firewall configuration is available for user inspection and modification. Firewall filtering functions are implemented by modules. Jetico Personal Firewall contains no hidden or compiled-in features.
-  **Low resources consumption.** Jetico Personal Firewall is designed to be high-performance and small footprint software.

Related info:

[How Jetico Personal Firewall protects the system?](#)

How does Jetico Personal Firewall protect the system?

Jetico Personal Firewall protects your computer from remote as well as outbound (trojan) attacks. It constructs filtering barriers between your computer and other networks. Jetico Personal Firewall uses unique triple-level filters and inspects every network related event in the system. [Read more about Jetico Personal Firewall filters...](#)

Firewall filters are controlled by rule sets. In order to achieve the ultimate level of security, filters must be properly configured. So firewall configuration issues should be considered as a vital part of your security system.

Jetico Personal Firewall's configuration approach is good both for beginners and advanced users.

- **Easy for beginners.** Jetico Personal Firewall works in self-learning mode by default. It displays a popup message when an unknown event happens. You should simply answer the question. So in most cases users won't have to explore firewall configuration internals. [Read more about Jetico Personal Firewall learning mode...](#)
- **Comprehensive for advanced users.** Jetico Personal Firewall provides full access to its configuration. Advanced users can analyze, modify or create their own configurations. [Read more about Jetico Personal Firewall configuration internals...](#)

Related info:

[Jetico Personal Firewall filters](#)

[Jetico Personal Firewall configuration](#)

[Learning mode](#)

Jetico Personal Firewall filters

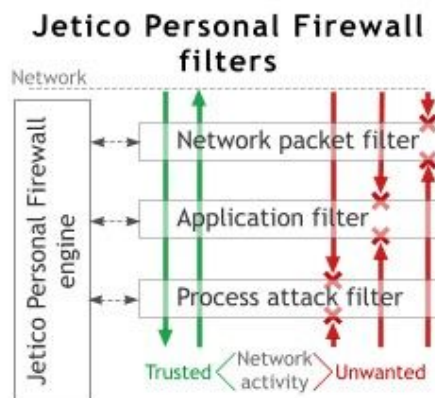
Jetico Personal Firewall installs three configurable filters at different layers of operating system.

- [Network packet filter](#) works at lower level. It processes packets coming to and from network adapter.
- [Application filter](#) is capable of filtering network connections on per application basis.
- [Process attack filter](#) is designed to prevent process hijacking.

Individual filters deal with different event types and could be considered as independent software components.

Each filter consists of two parts.

- The first part intercepts its own sort of events. For example, Network packet filter hooks network packets.
 - The second part checks the intercepted event according to [firewall configuration](#) and determines whether to allow or block it.
- The checking parts of filters are implemented as independent modules.



Please note also that Jetico Personal Firewall is not antivirus software. Jetico Personal Firewall gives you unprecedented control over network activity, but it does not protect your computer from viruses. If you need virus protection also please install third-party antivirus software.

Related info:

[Network packet filter](#)

[Application filter](#)

[Process attack filter](#)

Network packet filter

Filter purpose

Network packet filter helps to neutralize remote attacks, such as various port scans, packet bombs, etc. It is also used to permit or block specific protocols, services or address zones for your computer.

Filter domain

Network packet filter processes individual network packets. In current version only Ethernet frames are supported.

Operations

- Packet validity verification
- Packet parameters checking: source and destination addresses, protocol, direction, etc.
- Stateful inspection; Network packet filter can recognize packets that belong to authorized network sessions

Rule types

[Network protocol rule](#),
[IP rule](#)

Related info:

[Jetico Personal firewall filters](#)

[Network protocol rule](#)

[IP rule](#)

Application filter

Filter purpose

Application filter defines what network activity is allowed (or blocked) on per-application basis. It is applicable for blocking unknown or dangerous applications. For trusted applications it is used to assign a set of allowed network communications.

Since different computers run different software, Application filter uses [learning mode](#) to build rule set that meets your individual requirements.

Filter domain

Application filter processes network activity in conjunction with the application.

Operations

- Application checking
- Controlling access to network subsystem
 - **Access to network.**
'Access to network' is a separate event which means general access to networking subsystem preceding to all network communications.
While 'Access to network' is not enabled for an application, it won't be permitted to execute any network-related function.
- Connection parameters checking: local and remote addresses, protocol, connection type, etc.
- [Learning mode](#) operation

Rule types

[Application rule](#)

Related info:

[Jetico Personal firewall filters](#)

[Application rule](#)

Process attack filter

Filter purpose

Process attack filter is designed to protect your computer from outbound attacks. Many trojans try to identify themselves as legal applications to pass firewall. Process attack filter reveals and suppresses that activity.

Filter domain

Process attack filter monitors behaviour of all processes running in Windows and detects suspicious activity of some process.

Trojan and virus programs usually attempt to distribute themselves over network and hide their activity exploiting legal Windows functionality. Since some legal applications use the same services, [learning mode](#) is preferred for process attack filter.

Operations

- Application checking
- Functions checked:
 - **Installing system-wide Windows hook.**
This method was originally intended to allow hooker application process some events (keystrokes, mouse movement, etc.) before other applications do. Many legal applications use hooks: keyboard switchers, desktop managers... Even Internet Explorer installs system-wide hooks. Unauthorized programs use hooking technique to inject their code into trusted process and then execute it on behalf of trusted application.
 - **Starting an application with hidden window.**
Some application starts another one with hidden window. Using this simple trick unauthorized program can run invisible web browser and access the Internet. Launching an application with hidden window generally does not indicate an attack. This action is often performed by legal applications.
 - **Writing to other process' memory, Injecting code into other process, Modifying own child processes, Low-level access to system memory.**
These actions almost definitely indicate trojan/virus programs. All of them are employed to inject unauthorized code or data into trusted process.
- [Learning mode](#) operation

Rule types

[Process attack rule](#)

Related info:

[Jetico Personal firewall filters](#)

[Process attack rule](#)


Hash checking filter

Filter purpose

Hash filter acts as additional application integrity checking module.

Filter domain

Hash filter works on top of [Application](#) and [Process attack](#) filters.

All application and process attack events are checked by hash filter first. Thus  **accept** action will result in passing event to application or process attack filter for further processing.

Operations

- Application integrity checking
- [Learning mode](#) operation

Rule types

[Hash checking rule](#)

Related info:

[Jetico Personal firewall filters](#)

[Hash checking rule](#)

Jetico Personal Firewall configuration

Jetico Personal Firewall configuration is a set of rules which controls [firewall filters](#).

The main configuration unit is called **Security Policy**. It defines whether to allow or block particular network activity: incoming or outgoing connections, data transfer and even individual packets.

The security policy is an arranged set of atomic firewall rules. Jetico Personal Firewall uses very flexible and powerful table-based concept to construct security policy.

Jetico Personal Firewall is shipped with three prebuilt security policies. They provide different protection levels and should be used under specific circumstances.

- **Allow all** permits all inbound and outbound traffic as it were no firewall installed in your system. Please use it if you really need to run software conflicting with Jetico Personal Firewall. Remember that 'Allow all' policy does not provide efficient protection for your computer.
- **Optimal protection** is the security policy for everyday use. Initially it contains only the basic set of rules. 'Optimal protection' works in learning mode. Day by day it asks questions about emerging network activities and fills configuration up to meet your specific requirements.
- **Block all** blocks every network related event in your system. It makes network inaccessible. Use this policy in emergency cases when you see that your computer is under attack.

Related info:

[Choosing security policy](#)

[Advanced firewall configuration](#)

Learning mode

Jetico Personal Firewall starts to protect the computer just after installation. Initially it uses preconfigured security policy. Then the firewall configuration should be adjusted to meet your requirements. The simple way Jetico Personal Firewall does it is the **Learning mode**.

Learning mode allows you to build an efficient security policy without digging into Jetico Personal Firewall configuration internals.

Learning mode in action

When some application connects to the Internet and security policy does not have directions to process that event automatically, Jetico Personal Firewall displays the Popup message (see screenshot).

The Popup message reports about the particular network event. It displays events parameters and waits for user to define the verdict.

User's answer is stored into the security policy. It will be used to process forthcoming events automatically.



Related info:

[Choosing security policy](#)

[Popup messages and Learning mode](#)

System requirements

Jetico Personal Firewall system requirements

- Windows NT4sp6/2000/XP operating system
- 10 MB disk space
- Installed size is 5MB

Please note that some firewall or antivirus software vendors claim that their software is incompatible with other firewalls. Thus if you had installed such kind of software please uninstall it prior to Jetico Personal Firewall installation.

Uninstall details could be found in documentation supplied by software vendor.

Installing Jetico Personal Firewall

The easiest way to install and configure Jetico Personal Firewall system is to use the Setup program, supplied on the installation disk.

Setup program

Setup copies all necessary files to your hard disk and inserts required lines into the Windows Registry database.

To install the Jetico Personal Firewall, run **JPFWall.EXE**. It is recommended that you exit all Windows programs before running Setup program.

Jetico Personal Firewall setup uses the standard Windows way to install software and provides all necessary explanations of the installation's details. The only default information that the user may want to change during installation is the Program Folder name for the Jetico Personal Firewall program files and the Destination Directory name for where Jetico Personal Firewall files will be placed.

All dialog windows of the Setup programs have the following buttons:

- - click this button to abort installation
- - click this button to proceed with installation
- - click this button to return to previous step of installation

After a successful installation, Setup will ask you to restart your computer. This is because the Jetico Personal Firewall drivers will need to be loaded into the computer memory before you begin to use the Jetico Personal Firewall.

Note: The Jetico Personal Firewall setup program also writes information to the Windows Registry database, places low-level drivers in the Windows system directory, and prepares the file for the uninstall procedure.

How to uninstall Jetico Personal Firewall

If you need to uninstall Jetico Personal Firewall software please use Add/Remove Programs feature of Windows.

1. Launch Windows Control Panel from the **Start Menu**.
2. Select Add or Remove Programs in the **Control Panel**.
3. Select **Jetico Personal Firewall 2.0** item.
4. Click button to start uninstall program.

Note. It is recommended to exit running copy of Jetico Personal Firewall prior to starting uninstall program.

Starting and shutting down the firewall

Start

Jetico Personal Firewall is started automatically upon system startup.

If you stop Jetico Personal Firewall and want to start it again:

1. Check whether Jetico Personal Firewall is already started - simply check if [System tray icon](#). is displayed
2. Open Windows **Start menu** -> Programs
3. Select **Jetico Personal Firewall**
4. Click **Jetico Personal Firewall** menu item

Jetico Personal Firewall installation program adds Firewall main program to system startup list.

Shutdown

To shut Jetico Personal Firewall down:

1. Proceed to the [File menu](#)
2. Click **Shutdown firewall** menu item

or

1. Invoke the [Systray menu](#)
2. Click **Shutdown firewall** menu item

Related info:

[Jetico Personal Firewall user interface](#)

Jetico Personal Firewall configuration basics

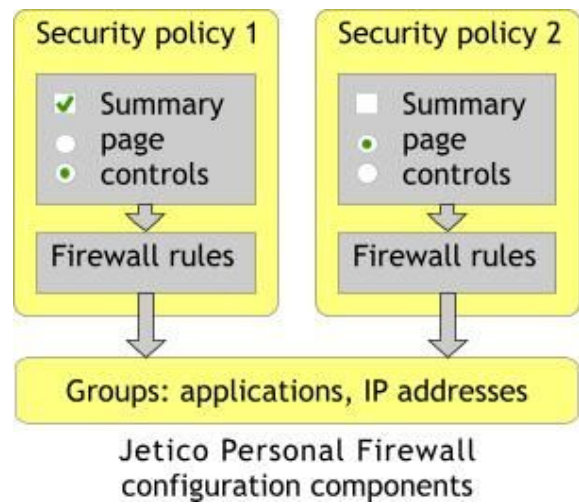
Jetico Personal Firewall offers different ways to adjust configuration to user's needs.

The simplest way is choosing the security policy. [Choosing security policy](#) chapter explains how to choose and apply suitable security policy.

The security policy has additional level of control available via policy's summary page. Summary page controls are programmed to enable or disable particular rules without ruleset modifications. Please refer [Using policy summary](#) chapter for details.

The next concept to pay attention too are firewall variables - groups. Firewall rules use groups as parameters for filtering. Currently two types of groups are supported: Application paths and IP address ranges. The user can modify such self-explaining variables as "Trusted zone", "Blocked zone" or "Web browser applications". See [Groups editing](#) chapter for details.

Finally, the user can edit the ruleset. Please note that understanding of network principles are required to compose and edit firewall rules. [Advanced firewall configuration](#) chapter is devoted to ruleset modifications.



Related info:

[Choosing security policy](#)

[Using policy summary](#)

[Groups editing](#)

[Advanced firewall configuration](#)

Choosing security policy

Security policy considerations

Jetico Personal Firewall is shipped with three preconfigured security policies.

- **Allow all** turns firewall protection off. Use it to resolve possible conflicts with Jetico Personal Firewall.
- **Optimal protection** provides ultimate protection level for your computer. Intended for everyday use.
- **Block all** cuts off your computer from network. This policy is for emergency use.

Setting security policy

To set firewall security policy:

1. Select appropriate security policy from the [Policy bar](#).

or

1. Click Right Mouse Button on Jetico Personal Firewall [System tray icon](#).
2. Select [Security policy... >](#) menu item.
3. Select appropriate security policy.

or

1. Select [Configuration explorer](#) tab.
2. At the left pane click Right Mouse Button on appropriate security policy root item.
3. Select [Apply policy](#) item of context menu.

Default security policy

When Jetico Firewall starts up, the **default security policy** is applied.

To assign the default security policy:

1. Select [Configuration explorer](#) tab.
2. At the left pane click Right Mouse Button on appropriate security policy root item.
3. Check [Set default](#) item of context menu.

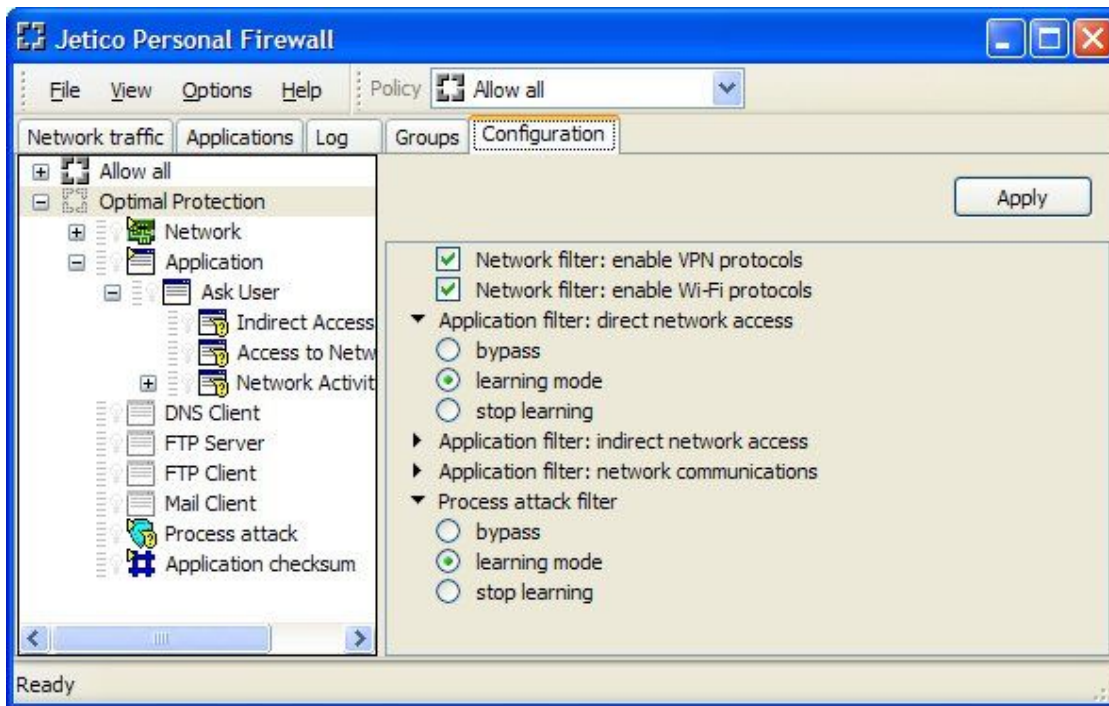
Related info:

[Jetico Personal Firewall system tray icon](#)

[Policy bar](#)

[Configuration explorer](#)

Using policy summary



Jetico Personal Firewall v2 introduces summary page for each security policy (see screenshot). To view summary page open **Configuration** tab and select policy root item at the [left pane](#).

Checkboxes and radio buttons on the summary page enable or disable some rules from selected security policy. If corresponding rules were enabled/disabled directly and firewall can't compare it with control states corresponding control will be grayed.

The default "Optimal protection" policy uses following scheme for controls. Each learning mode rule receives tri-state control:

- **bypass** - accept all events processed by filter
- **learning mode** - turn on learning mode; ask user about unknown events
- **stop learning** - turn off asking rule; use learned data for filtering

In addition, it provides controls for enabling VPN and Wi-Fi protocols (disabled by default).

Groups editing

To edit group values do following actions:

1. Select [Groups explorer](#) tab.
2. Select desired group type in the Group explorer's left pane.
3. Group explorer's right pane displays the list of available groups.
4. Select group to modify
5. Double-click on selected group or press **Enter** or call right pane's context menu by clicking Right Mouse Button, then select **Edit** menu item.
6. [Group editing dialog](#) will be brought up to you. Please edit and press **OK** to accept or **Cancel** to decline changes.

Group values format

Firewall rules use group values as they were typed in to corresponding rule editor field.

- Valid **Application paths** are fully qualified file names. '?' and '*' wildcards are also allowed. Example: *C:\Windows\telnet.**
- **IP address** ranges are accepted in x.x.x.x-y.y.y.y form. x.x.x.x is the first IP address of a range, y.y.y.y is the last one.

Related info:

[Groups explorer](#)

Popup messages and Learning mode

The following chapters describe Jetico Personal Firewall Learning mode. They provide general information about Learning mode and explain different types of Popup messages. Recommendations on answering the Popup messages are also given.

- [What is Learning mode?](#)
- [Answering popup message.](#)
- [Notes on event types.](#)
- [Application rule popup parameters](#)
- [Process attack rule popup parameters](#)
- [Hash checking rule popup parameters](#)

What is Learning mode?

Jetico Personal Firewall filters network traffic according to Security policy chosen by the user. Conventional firewall rules either drop or pass network events depending on filter settings. Once configured firewall can recognize and prevent a number of network attacks automatically. For example, it can drop "bad" low-level network packets that may have inconsistent structure and harm your computer. Besides of this, the firewall is aware about network activity of standard Windows services and allows the services to perform the only tasks they are intended for.

From the other hand, the user may have a number of software installed on his/her computer that also access the Internet. The firewall has to decide whether such a program is a trusted application, or it is a trojan attempting to make network connection illegally. Such cases require user's attention.

Jetico Personal Firewall uses **Learning mode** to solve this problem. Learning mode rules have special action - "ask". When an event meets the rule's condition the firewall displays popup message. The message reports about event details and offers multiple choice answer to the user. The user's answer will modify firewall configuration an next time such event will be processed automatically.

Related info:

[Jetico Personal Firewall configuration](#)

Answering popup message

Popup message dialog (see screenshot) consists of two parts:

- **message text** at the top and
- **answer options** at the bottom of dialog

Message text

Message text contains information about event triggered the popup. Text body is produced from template by actual parameter values substitution. Substituted parameter values are underlined. Individual rules can have their own message templates to make resulting text more informative. Message templates can be changed in the rule editor dialog.

Show rule that sent this popup is a link to rule that fired the popup. If you click the link Jetico Personal firewall will display [Configuration explorer](#) with target rule selected.

Answer options

In the learning mode firewall fires pouts on some network-related events and modifies ruleset according to user action. Popup message dialog offers variable set of answers. The number of available answers may vary: firewall administrator can protect firewall configuration and only **Allow once** and **Block once** will be shown.

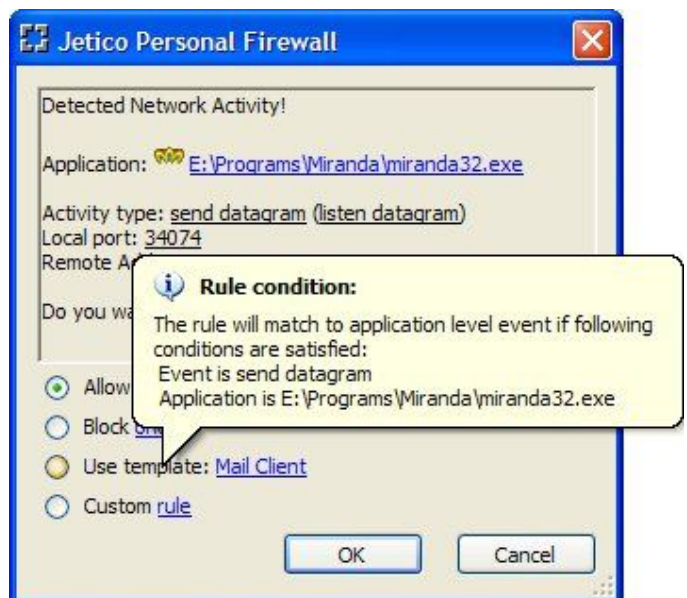
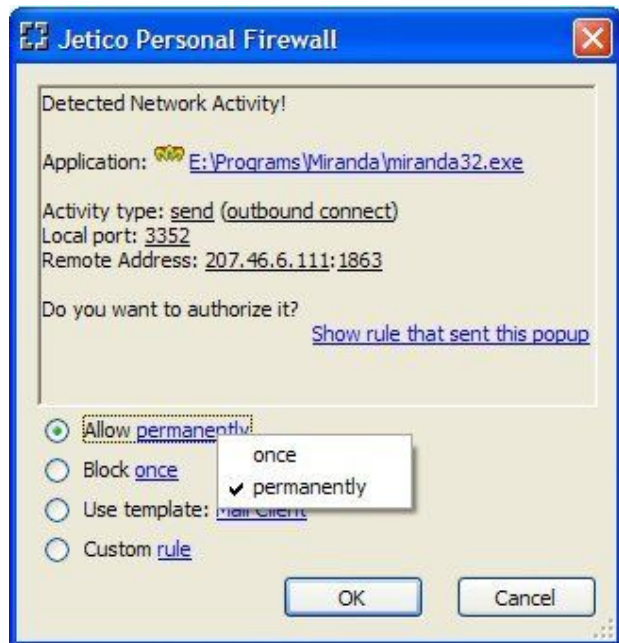
The user makes choice by selecting an appropriate radio button. Answers may have additional settings accessible via link-style part.

If selected answer requires firewall to modify configuration, popup message will display tooltip with the text of rule to be created (see screenshot below).

To approve your selection click

Here is the list of answer options:

- **Allow permanently** - firewall will create permissive rule. Use this answer if you do trust corresponding application.
- **Allow once** - allow specific actions while application instance is active. The answer is suitable for trusted applications that require to be executed once. Setup and registration programs fall into this category.
- **Block permanently** - create blocking rule. This answer should be selected if you see that the application (even trusted one) is doing wrong. For example, if your mail reader is trying to access non-mail ports you'd better deny it.
- **Block once** - block specific actions while application instance is active. Use this answer if you are not sure about application activity.
- **Use template: + template_name** - create rule which will pass event to selected template table. This answer is the best choice for well-known application. Template tables



contain predefined rules for them. As a result, the number of popups will be minimized.

- **Custom rule** - create custom rule; the user is allowed to edit all rule parameters. For advanced users. Use this option if you feel that options above are not suitable.

Notes on event type

Application level events

1. **access to network**
It is a general event occurred before the application actually sends or receives some packets to network. At that time the application just loads Windows modules necessary to access network.
2. **indirect access to network**
Application does not use networking components directly. Instead, it forces another application to perform network-related job.
3. **inbound/outbound connection**
The program attempts to create outbound connection or accept inbound connection. Please draw your attention on addresses and ports if possible. Trojans and other malicious programs scripts can force trusted applications to establish unauthorized connections with suspicious peers.
4. **send/receive datagram.**
Reported program attempts to send or receive network datagrams. Please use the same considerations as it is advised above to make a right decision on the event.

Process attack level events

Trojan and virus programs usually attempt to distribute themselves over network and hide their activity exploiting legal Windows functionality. Since other trusted applications may also use the same Windows mechanisms, Jetico Personal Firewall needs in a user attention to make a final decision on the running process.

Jetico Personal Firewall monitors behaviour of all processes running in Windows and detects actions considered potentially suspicious. Following events are reported:

1. **install global hook**
Windows program can register specially designed procedure (so-called "hook") to be called when some event in the operating system occurs. For example, when the user presses key on keyboard or moves the mouse. It is interesting that to work properly, Windows must load the Hook procedure into the memory of all programs running in Windows (more correctly, all programs that have graphic user interface).

Windows hooking mechanism is used both by legal applications and trojans. As soon as trojan installs Windows hook, it can access network in its hooking procedure. Since the hooking procedure is in the memory of other legal process (for example, in Explorer.exe process), the user will not realize that network is accessed by the trojan.
2. **create hidden window**
Trojan program can run another trusted application and make the application accessing network. For example, Internet Explorer can be run in that way. Of course, the user will notice that something is going wrong if he/she sees unexpectedly appeared Internet Explorer's windows. So the trojan program can simply run Internet Explorer's windows in hidden mode.

Jetico Personal Firewall reports about the event, but please note that legal programs often run their modules with hidden windows, for example, when such a module supports icon in the system tray. Please pay attention to the application name reported in the firewall popup message and allow the trusted application proceed with its activity.
3. **write to application's memory**
Trojan program can modify memory of another trusted application. Usually trojan replaces contents of memory where legal code of the trusted application resides by the code of the trojan's procedure that accesses network. As soon as the procedure runs, it accesses network so that everything looks like the trusted application itself decides to access network.
4. **create remote thread**
When Windows application runs, it may have one or several so-called "threads". Every thread works in parallel with other threads and executes its own code in the context of the application's process.

Windows allows remote thread creation, i.e. one process can create thread that will work on behalf of another trusted process. In this case Windows believes that this trusted process is responsible for everything that the remote thread makes.

Trojan programs can use the technology of remote threads to hide their activity.
5. **modify child process**
Trojan program (attacker) can run another trusted application and modify its memory before the process of trusted application will run. Since the trusted process is not running yet, it may be difficult

to detect after some time that the trusted application will run the code of trojan program.

6. **direct memory access**

Trojan program can harm loaded Windows system modules or running applications by modifying contents of system physical memory. Since the physical memory is common for all the processes running on the computer, such a dangerous program can make any process doing what the trojan program wants. Windows security mechanisms normally does not allow programs to make such a trick, but it is still possible. If Jetico Personal Firewall detects this kind of attack, it definitely means that the reported program is a trojan.

Hash checking events

Hash checking module acts as supplemental frontend to Application and Process attack filters. It intercepts both Application and Process attack events.

1. **access to network**

Corresponds to application **access to network** event.


2. **indirect access to network**

Corresponds to application **indirect access to network** event.

3. **network communications**

Includes all remaining events.

How to find rules added by Popup messages

Jetico Personal Firewall [Popup messages](#) are triggered by rules with **ask user**  action.

When you make your choice and press appropriate rule is created. The newly created rule is placed just before the **ask user** rule. So all rules added in learning mode are residing in tables with **ask user** rules.

Optimal protection is the only security policy with learning mode supplied by Jetico. If you got stuck with you configuration, please take a look at '**Ask user**' and '**Process attack table**' tables. These tables contain all changes made to configuration in learning mode.

Please note that Popup message provides information about source table.

Monitoring network traffic

Why network traffic monitoring is important?

Remember that there are no other ways to communicate with the Internet than via network packets. Thus traffic monitoring gives authentic view on network communications.

To watch network traffic information, select the [Traffic monitor](#) tab of the Jetico Personal Firewall main window. It presents both graphs and statistics in realtime.

Traffic monitor information should be used mainly for an estimation. Take a notion of [Event logging](#) if you need a precision tool.

Related info:

[Traffic monitor](#)

Monitoring applications

To watch applications' networking activity, select the [Applications monitor](#) tab of the Jetico Personal Firewall main window. It displays network connections information grouped by application in realtime.

Applications monitor information should be used mainly for an estimation. Take a notion of [Event logging](#) if you need a precision tool.

Related info:


[Applications monitor](#)

Event logging

Jetico Personal Firewall logging subsystem is able to record any event handled by firewall.

Every firewall rule has **Log level** parameter. It controls whether to log or not the event which has triggered the rule. So when you want to analyze network packets or connections you only need to select appropriate firewall rule and turn logging on.

How to log events?

1. You may either use existing rule or create new to make log sensor. If you have created new rule you'd better use **continue**  action to leave existing configuration unaffected.
2. [Edit](#) selected rule's condition. Please remember that only events matching the rule will be logged.
3. Set **Log level** parameter to non-'disabled' value. Log entries with different levels are displayed in different colors.
4. Apply modified security policy
5. Switch to [Log monitor](#) to watch fresh log entries.

Log options

Jetico Personal Firewall log options are accessed via **Options->Log...** (see [Main menu](#)) Following options are available to control the logging subsystem:

- Folder where log files will be stored. Jetico Personal Firewall logging subsystem will write data to sequential files in selected folder.
- Log file size upper limit.
- How many latest log files should be kept. Older log files will be deleted automatically to save your disk space.

Viewing log files

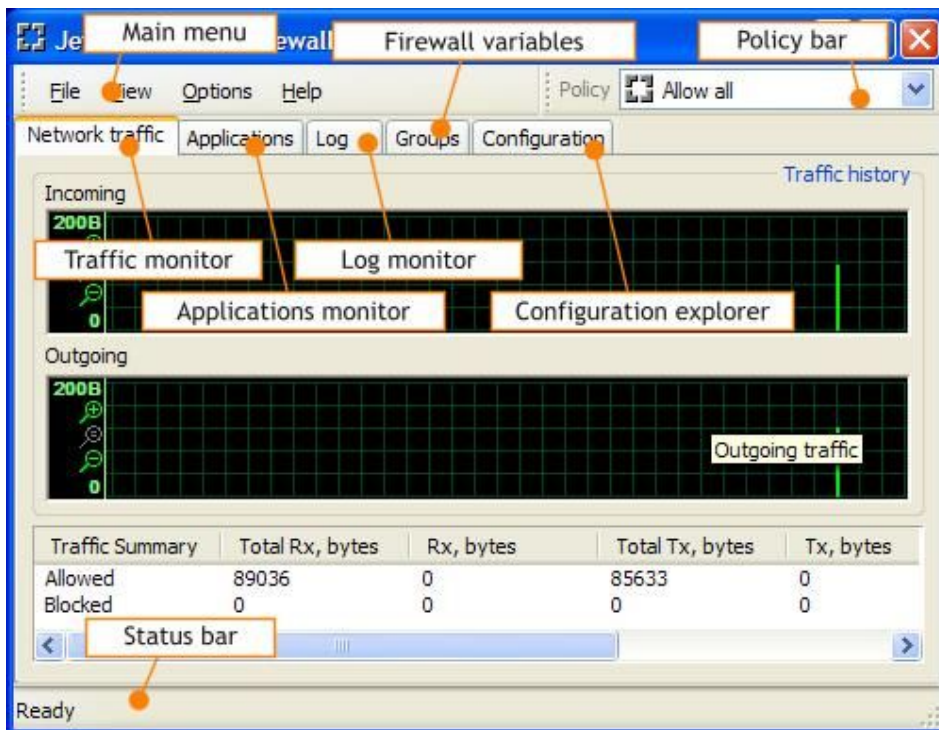
To view external log file:

1. Select [Log monitor](#)
2. Invoke [Log monitor context menu](#)
3. Click **Select log file..** item, then select log file in 'Open' dialog.

Related info:

[Log monitor](#)

Jetico Personal Firewall Main window



The Jetico Personal Firewall main window contains (see screenshot):

- [Main menu](#)
- [Policy bar](#)
- [Traffic monitor](#)
- [Applications monitor](#)
- [Log monitor](#)
- [Groups explorer](#)
- [Configuration explorer](#)

More detailed information on each of the elements will appear later in this guide.

Command bars



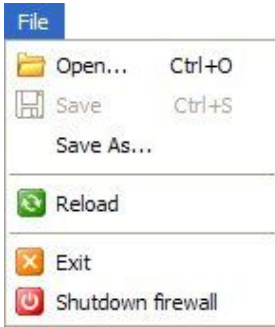
[Main menu](#)

[Policy bar](#)

Jetico Personal Firewall command bars - [Main menu](#) and [Policy bar](#) span along the top of the main window.

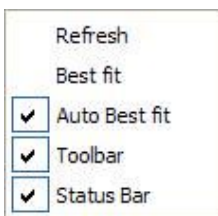
Main menu

File



- **Open** - load security policy from selected file
- **Save** - save changes
- **Save as** - write selected security policy to another file
- **Reload** - update firewall configuration
- **Exit** - terminate Jetico Personal Firewall user interface functions; network protection level will not change
- **Shutdown firewall** - stop firewall protection service

View



- **Refresh** - update the current tab contents
- **Best fit** - resize columns in the current tab so that all information will fit into them
- **Auto Best fit** - toggle "Best fit" mode
- **Toolbar** - hide or show the toolbar
- **Status bar** - hide or show the status bar

Options



- **General...** - show general options dialog
- **Log...** - show log options dialog
- **Access control...** - show firewall access control options dialog

Help



- **Contents...** - display this help
- **About...** - show Jetico Personal Firewall program information
- **Registration** - show product registration dialog
- **Send order** - opens Jetico product order page in the web browser

Policy bar



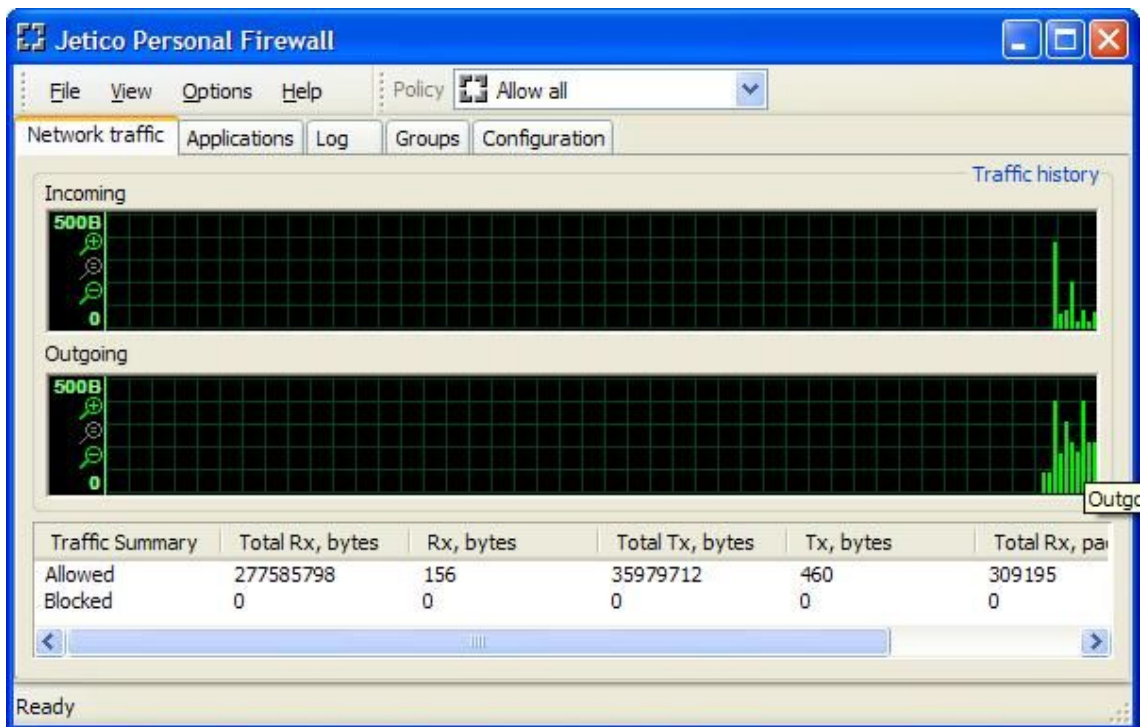
Policy bar contains single control - **policy chooser** combobox.

Policy chooser is designed to manage security policies. It combines the following functions:

- Selection marks current security policy.
- Use combobox selection to apply desired security policy.
- Drop-down list contains list of available security policies.

Traffic monitor

Traffic monitor shows both incoming and outgoing network traffic graphs for your computer in realtime. In addition, summary statistics is shown.



Traffic graphs

Incoming and outgoing traffic graphs monitor network traffic in realtime. Graph scale is tracked automatically in dependence on displayed values.

- **Red** denotes blocked traffic
- **Green** denotes allowed traffic

Traffic graph controls



Zoom in. When largest zoom factor is reached control disabled and grayed.



Automatic zoom. Traffic graph will be scaled automatically according to data displayed. In automatic zoom mode control is disabled and grayed.

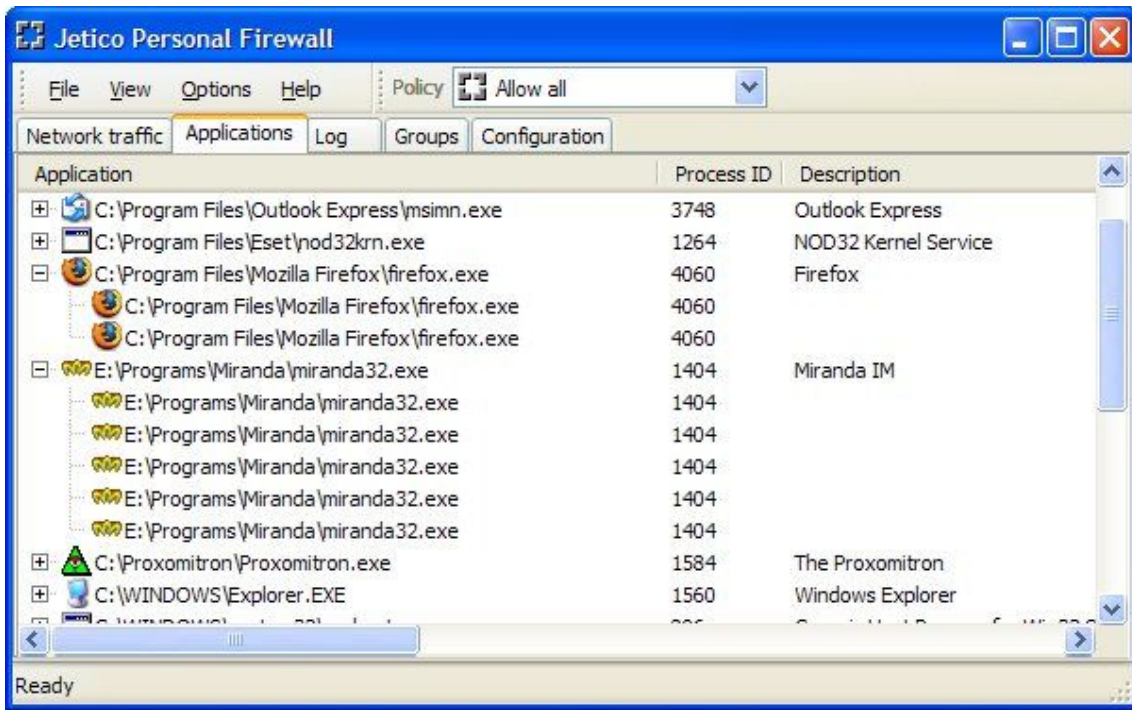


Zoom out. When smallest zoom factor is reached control disabled and grayed.

Summary statistics

Summary statistics display grand total incoming and outgoing traffic since power up in bytes. Summary discern allowed and blocked events as well.

Applications monitor



Applications monitor displays list of applications connected to network. It provides detailed information about open sockets/connections.

Please note that some applications listed in Applications monitor have no active connections. These applications have initialized network subsystem and became able to perform name domain lookup or retrieve information on local network adapters.

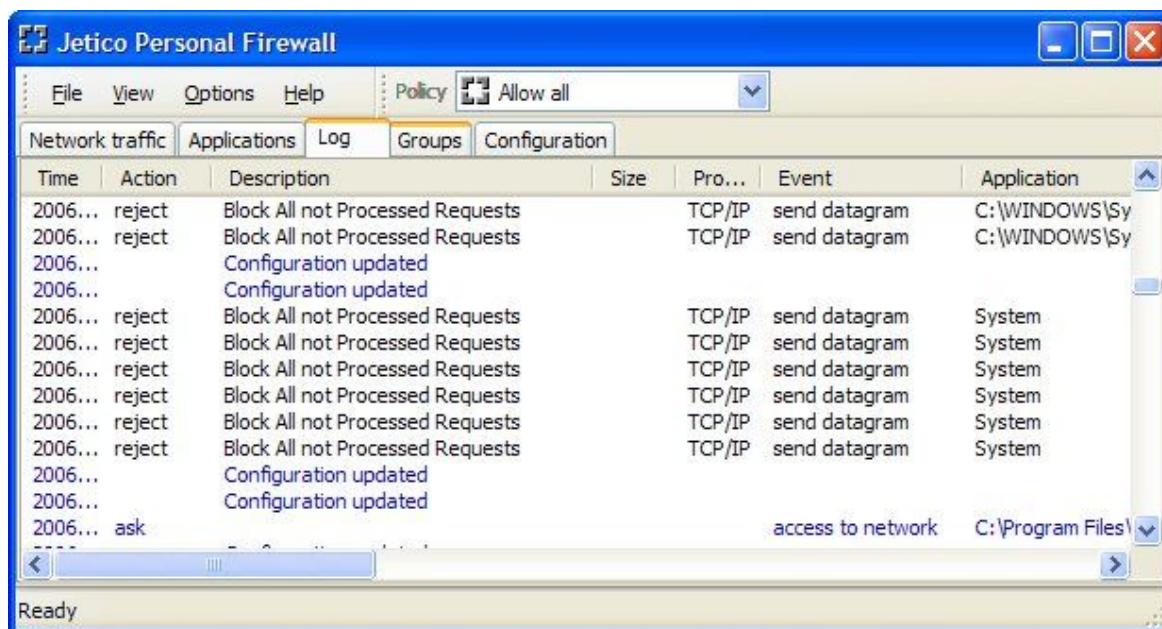
Applications monitor context menu

Properties
Copy text
Collapse
Terminate process

Applications monitor context menu contains following items:

- **Properties** - invoke system shell 'Properties' dialog for selected application's main module
- **Copy text** - copy selected text lines to clipboard
- **Expand (Collapse)** - expand (collapse) active sockets and connections list for selected application
- **Terminate process** - terminate selected application; be careful when using this function

Log monitor



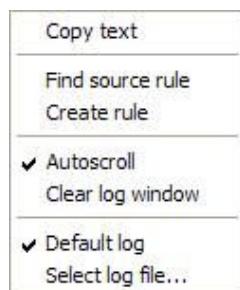
Log monitor window displays Jetico Personal Firewall log messages in real-time. Log messages indicate firewall system health to you.

Messages of different severity levels are marked by different colors - from blue (informational) to red (alerts).

Log grows downward so recent messages appear at the bottom.

Right mouse click on Log monitor's window elements will invoke corresponding context menu - Log context menu or Log header context menu.

Log context menu



Log window context menu contains following items:

- **Copy text** copies selected text lines to clipboard.
- **Find source rule** available on log entries produced by firewall rules. Find corresponding rule.
- **Create rule** create new rule with condition taken from log entry.
- **Autoscroll** (checkable). When checked, log messages are scrolled automatically so that the latest message is always visible. When unchecked, currently selected message retains its position.
- **Clear log window**. Clears current log window contents.
- **Default log** (checkable). When checked, the contents of active log is displayed.
- **Select log file**. Brings up dialog to select log file to display. Selected log file will be added to **log files MRU list**.

Log header context menu

- ✓ Action
- ✓ Description
- ✓ Size
- ✓ Protocol
- ✓ Event
- Attacker
- ✓ Source address
- ✓ Destination address
- ✓ Source port
- ✓ Destination port
- ✓ Application
- ✓ Local address
- ✓ Remote address
- ✓ Local port
- ✓ Remote port
- ✓ Misc

Log header context menu allows the user to show or hide particular log columns. Log columns are explained below.

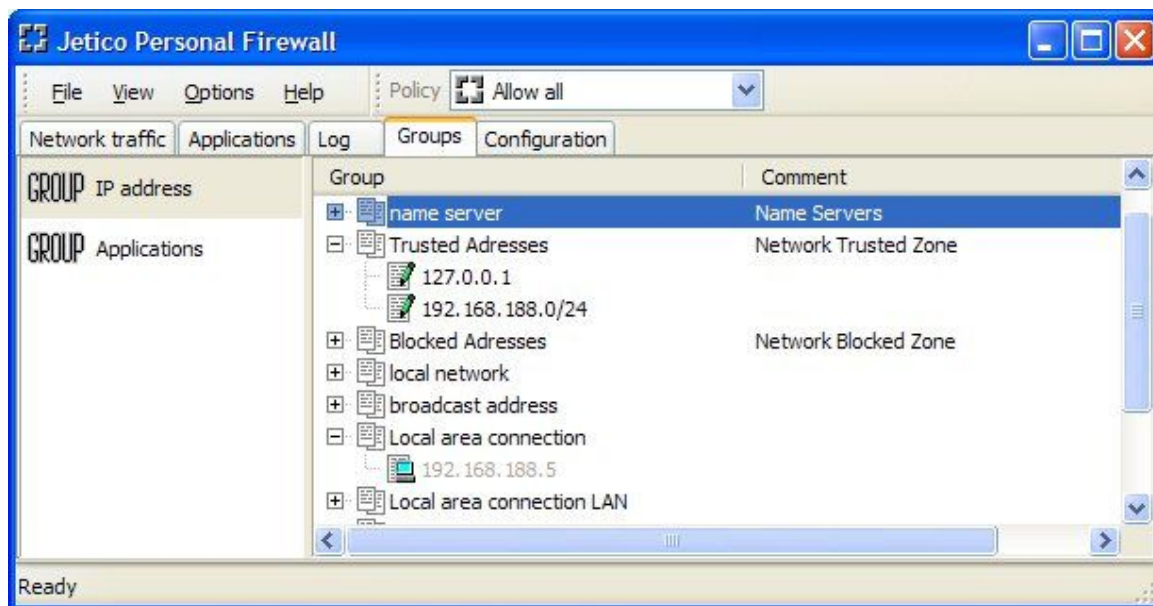
- **Time** - event registration time
- **Action** - firewall action taken on event

Optional fields

- **Description** - event description
- **Size** - data size, if applicable; e.g. network packet size
- **Protocol** - corresponding protocol; e.g. TCP
- **Event** - event type, such as network packet direction or connection status
- **Attacker** - intruder's address or other identity, if applicable
- **Source address** - source address of network packet
- **Destination address** - destination address of network packet
- **Source port** - source port of network packet; applicable to TCP and UDP packets only
- **Destination port** - destination port of network packet; applicable to TCP and UDP packets only
- **Application** - application initiated network communications, if applicable
- **Local address** - address at network communication's local end
- **Remote address** - address at network communication's remote end
- **Local port** - port at network communication's local end
- **Remote port** - port at network communication's remote end
- **Misc** - miscellaneous not covered by fields listed above

Groups explorer

Groups explorer provides access to Jetico Personal Firewall variables - groups. Groups can be used by firewall rules as parameter values.



Left pane

Left pane displays list of group types. Current version supports two types only: Application path and IP address range. Groups of selected type are displayed in the right pane of the Groups explorer.

Right pane

Right pane lists groups of selected type. The user can expand and view group values by clicking "+" image near group name. Each group can contain both automatic and user-defined values.

Group icons

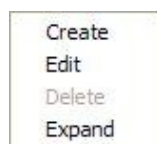


- value retrieved from system configuration automatically.



- user-defined value.

Right pane context menu



Context menu contains following items:




- **Create** - create new group.
- **Edit** - edit selected group.
- **Delete** - delete selected group.
- **Expand** - expand group contents.

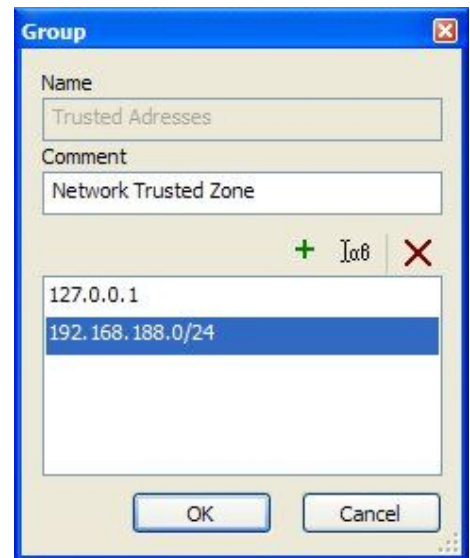
Group edit dialog

Group edit dialog is brought up whenever user creates or changes existing group.

Group name can be altered when creating group only.

Dialog buttons:

-  - add new value
-  - edit selected value
-  - delete selected value



Configuration explorer

Configuration explorer allows user to browse, inspect and edit Jetico Personal Firewall configuration. Configuration explorer window is split into two panes.

- Left pane, the [Security policy view](#), operates at Security policy table level. Security policy view allows the user to:
 - Browse the Security policy structure
 - [Set active Security policy](#)
 - Assign the [default Security policy](#)
 - Add and remove tables
 - [Copy or move tables](#)
- Right pane displays either the [Policy summary](#) or the [Table view](#) depending on active item in the Security policy view.

Policy summary contains configurable controls for quick policy adjustment.

The table view provides access to firewall rules within the table selected in the Security policy view.

Table view's main functions are:

- Viewing table contents
- [Monitoring rule activity](#)
- Firewall rules operations: [add](#), [delete](#), [edit](#), [copy](#), [reorder](#).

Related info:

[Security policy view](#)

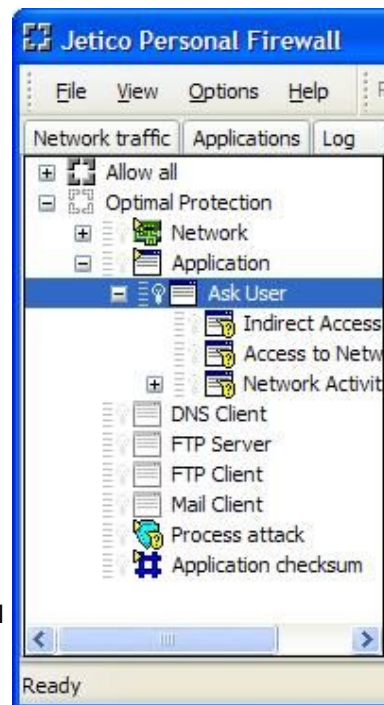
[Policy summary](#)

[Table view](#)

Security policy view

Security policy view is intended to control Jetico Personal Firewall at Security policy and table levels. Common operations include setting current security policy, creating, copying and deleting tables, Security policy structure navigation.

Security policy view displays security policy structure as a tree (see screenshot). All operations are accessible via context menus or by mouse operations on marked elements.



Security policy view icons

Security policy icons.

Active security policy. This policy is in effect now.

Inactive security policy.

Table icons.

[Network packet filter](#) table. Rules in this table must be capable of network packet processing. Currently [IP rules](#) and [Network protocol rules](#) are suitable for Network packet filter table.

[Application filter](#) table. Corresponding rules process application level network events. Currently [Application rules](#) are suitable for Application filter table.

[Process attack filter](#) table. Rules for unwanted process activity filtering should be placed here. Currently [Process attack rules](#) are available for Process attack filter table.

Table for [hash checking rules](#).

Icon modifications:

yellow arrow indicates **root table**. Rule processing starts here.

question mark indicates that table contains rules with **ask** action.

grayed icon means that firewall control paths do not reach that table and its rules are not processed.

Activity monitor icons.

No activity detected

1-10 hits

11-100 hits

101-1000 hits

1001-10000 hits

more than 10001 hits

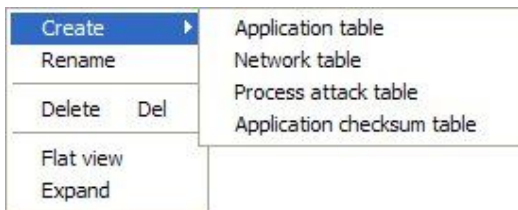
Security policy view context menus

Context menu for Security policy:



- **Apply policy** - set Security policy
- **Set default** - assign default Security policy. The default Security policy is applied upon firewall startup
- **Rename** - rename Security policy
- **Create...** - add empty table of particular type to the selected Security policy
- **Flat view** - switch between flat (simple table list) and hierarchical Security policy display
- **Expand** - expand current tree node

Context menu for tables:



- **Create...** - add empty table of particular type to the selected Security policy
- **Rename** - rename table
- **Delete** - delete table. If table is referred to, it can't be deleted, so 'Delete' item is grayed
- **Flat view** - switch between flat (simple table list) and hierarchical Security policy display
- **Expand** - expand current tree node

Policy summary

Summary view is displayed when policy root icon is selected in the [Policy view](#) (right pane). Summary view contains configurable checkbox and radio button controls for quick policy settings adjustment.

Controls are associated with particular firewall rules. When the user changes control state, corresponding rules are enabled or disabled.

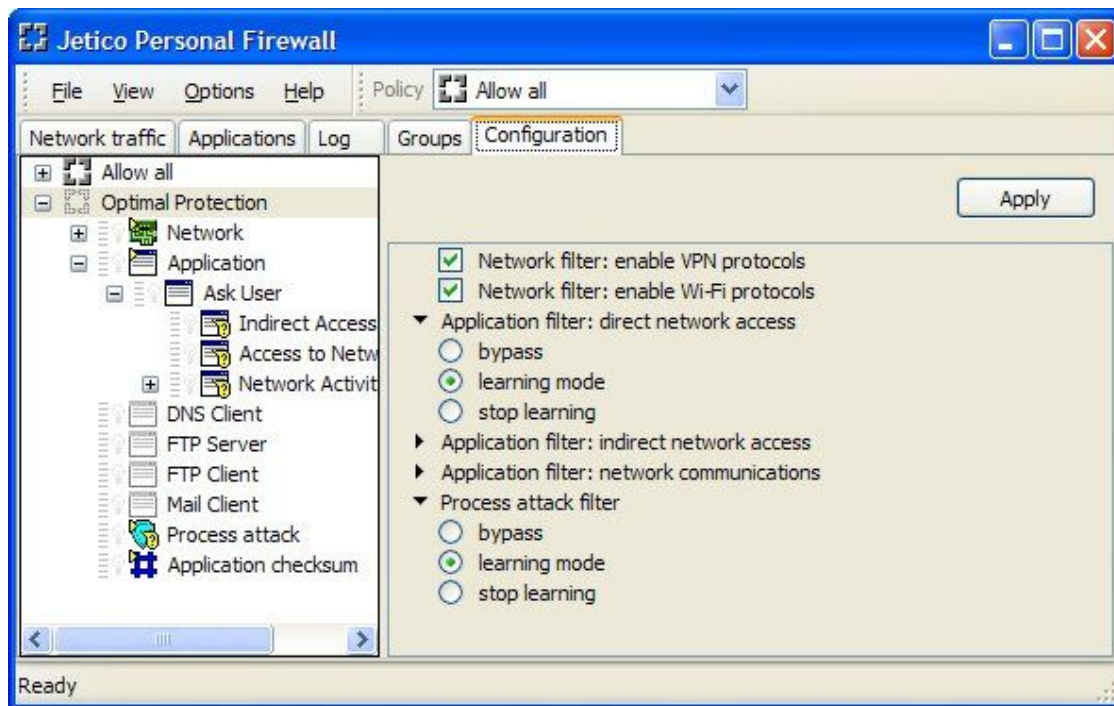


Table view

Table view provides access to firewall rules within the table selected in the [Security policy view](#). It displays table contents, one firewall rule per line (see screenshot).

Rule parameters set as well as table header columns set depend on [firewall table type](#). Indeed, [Network packet filter](#), [Application filter](#) and [Process attack filter](#) process different events with different parameters.

All rule functions are accessible via context menus or by mouse operations on selected elements.

Drag'n'drop operation is also available (refer to [Copying and moving rules](#) chapter).

Action	Activity	Description	Log level	Pro...	Direction	Application
Application...	Zone		disabled	TCP/IP	any	
<input checked="" type="checkbox"/> Application...	Zone		disabled	TCP/IP	any	
<input checked="" type="checkbox"/> accept			disabled	any	listening datagrams	
<input checked="" type="checkbox"/> accept			disabled	any	listening port	
<input checked="" type="checkbox"/> accept		Allow DNS requests	disabled	TCP/IP	send datagrams	
<input checked="" type="checkbox"/> accept		Allow DNS requests	disabled	TCP/IP	receive datagrams	
<input checked="" type="checkbox"/> Ask User			disabled	any	any	
<input checked="" type="checkbox"/> reject		Log All not Processed ...	alert	any	any	
<input checked="" type="checkbox"/> continue		Default action				

Table view icons

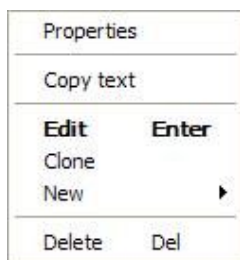
■ Rule state icons.

- Rule is enabled
- Rule is disabled and simply skipped
- The state of table's default action is always **Enabled** and could not be changed.
- An error occurred during rule loading. Hence rule is not loaded and has no effect.

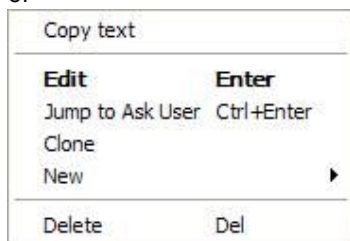
■ Activity monitor icons.

- No activity detected
- 1-10 hits
- 11-100 hits
- 101-1000 hits
- 1001-10000 hits
- more than 10001 hits

Table view context menu



or



- **Properties** - invoke application Properties dialog. Available if underlying text is valid application path
- **Copy text** - copy selected lines to clipboard as text info
- **Edit** - edit rule
- **Clone** - insert the copy of rule
- **New >** - invoke rule type submenu to select the type of rule to be created
- **Delete** - delete rule
- **Jump to ...** - navigate to child table. Available if underlying text is **go to table** action

Table view header context menu

Table header context menu allows the user to select which columns (rule parameters) to display. Rule parameters are explained below.

Menu items depend on selected table type. The one shown here is for Application filter table.



- **Activity** - rule activity rate
- **Action** - rule action
- **Description** - rule description
- **Log level** - rule logging level
- **Size** - data size, if applicable; e.g. network packet size
- **Protocol** - corresponding protocol; e.g. TCP
- **Event** - event type, such as network packet direction or connection status
- **Attacker** - intruder's address or other identity, if applicable
- **Source address** - source address of network packet
- **Destination address** - destination address of network packet
- **Source port** - source port of network packet; applicable to TCP and UDP packets only
- **Destination port** - destination port of network packet; applicable to TCP and UDP packets only
- **Application** - application initiated network communications, if applicable
- **Local address** - address at network communication's local end
- **Remote address** - address at network communication's remote end
- **Local port** - port at network communication's local end
- **Remote port** - port at network communication's remote end
- **Misc** - miscellaneous not covered by fields listed above

Popup message

Popup message (see screenshot) is displayed when firewall is configured to ask user upon particular network events.

The user is expected to choose appropriate answer option, then click .

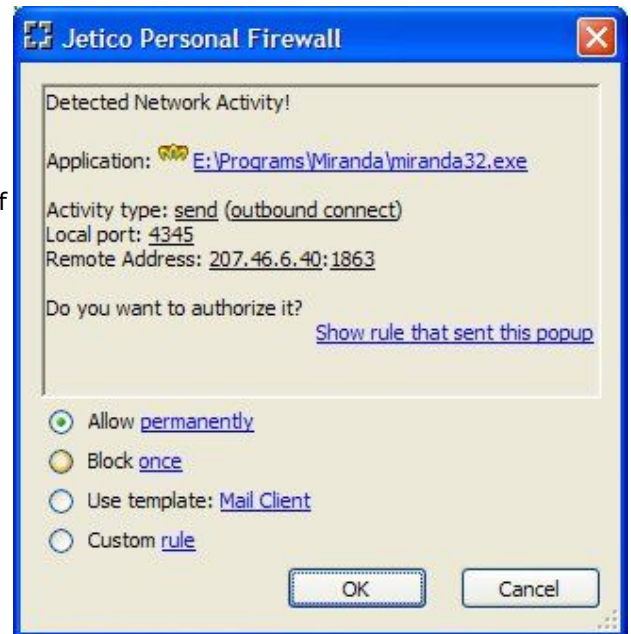
The top half of message dialog contains the description of event.

The bottom half of popup message window offers several answer options.

Detailed popup dialog description is available in the [Answering popup message](#) chapter.

Related info:

[Answering popup message](#)



System tray icon







System tray icon is displayed at the right (bottom) side of the Taskbar when Jetico Personal Firewall user interface is started.

The icon renders basic information about network traffic and current security policy as well as gives access to firewall control functions.

The active security policy name is displayed in the tooltip when cursor hovers Jetico Personal Firewall system tray icon.



The system tray icon image legend is shown below.

-  Incoming network traffic was allowed.
-  Some packets of incoming network traffic were blocked. If there were both allowed and blocked events, red arrow is rendered
-  There were no incoming network events
-  Entire outgoing network traffic was allowed.
-  Some packets of outgoing network traffic were blocked. If there were both allowed and blocked events, red arrow is rendered
-  There were no outgoing network packets

System tray icon context menu

Context menu is accessible via right mouse click on system tray icon image.



System tray icon context menu contains following items:

- **Restore** invokes Jetico Personal Firewall Main window.
- **Security policy** provides an easy way to switch firewall configuration.
- **About** shows Jetico Personal Firewall program information.
- **Exit** terminates Jetico Personal Firewall user interface functions. Network protection level will not change.
- **Shutdown Firewall** stops firewall protection service.

Advanced firewall configuration

Once installed to your computer Jetico Personal Firewall should be properly configured to provide the highest protection.

This chapter contains roadmap to information on Jetico Personal Firewall configuration.

General information

- [Firewall rules and tables](#)
- [Firewall rules processing](#)
- [Firewall configuration guidelines](#)

Jetico Personal Firewall rule types

- [Network protocol rule](#)
- [IP rule](#)
- [Application rule](#)
- [Process attack rule](#)
- [Hash checking rule](#)

Modifying configuration

- [Creating new rule](#)
- [Rule editing](#)
- [Enabling and disabling the rule](#)
- [Deleting the rule](#)

- [Copying and moving rules](#)
- [Copying and moving tables](#)
- [Creating template for Popup message \(Handle as...\)](#)

Firewall rules and tables

Jetico Personal Firewall filters network traffic according to the rules that block or allow your computer sending/receiving network packets.

Every firewall rule is a basic configuration unit that consists of the rule's parameters and verdict. The firewall compares parameters of the rule with parameters of network packet. If the rule concerns that network packet, the firewall blocks or accepts the network packet according to the verdict of the rule.

Group of rules can be united into table. The table may contain rules of definite type, for example, table of rules that are used to analyse consistency of low-level Ethernet packets.

Besides of this, some set of rules can be combined into table, because the rules are used to check some definite way of network packets' flow. For example, to check a proper behaviour of Web browsing application.

Table structure of rules used in Jetico Personal Firewall allows the software:

- minimize memory space inside the firewall modules to store the rules;
- increase performance of the firewall, because the firewall iterates hierarchial structure of tables instead of processing plain sequence of rules;
- make evaluation and modification of the rules' set by the user easier.

Please note that the firewall processes rules one by one until the program finds the rule with parameters corresponding to parameters of the analysed network packet. As soon as such a rule is found, the firewall blocks or accepts the packet according to the rule's verdict. After that the firewall stops processing its rules' set.

It means that order of rules plays significant role in Jetico Personal Firewall configuration. Please pay attention to the order for the rules with a close list of parameters.

Firewall rules processing

Jetico Personal Firewall filters network packets according to the firewall rules. Different types of the rules are united into different tables. Refer to [Firewall rules and tables](#) to get information about tables and rules. The set of Jetico Personal Firewall rules arranged into tables is called the firewall Security policy .

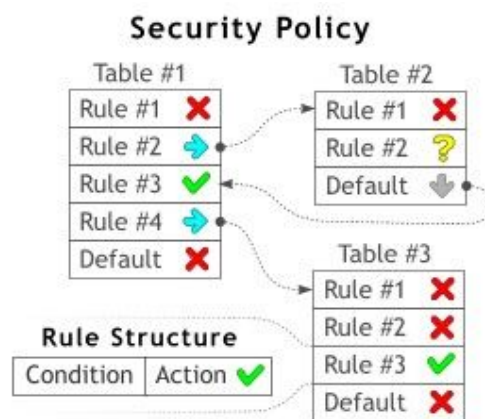
As it is mentioned in [Jetico Personal Firewall configuration](#) chapter, current version of the firewall is shipped with three predefined Security policies: 'Allow All', 'Block All' and 'Optimal Protection'.

Please note that Jetico Personal Firewall processes different types of network events with different filters (refer to [Jetico Personal Firewall filters](#) for details). As a result, different types of rules are provided for different network events.

Rule structure

As it is shown on the picture, every firewall rule consists of Condition and Action parts:

- **Condition** is a set of parameters that the firewall compares with parameters of network packet being processed at the moment. These parameters may include remote address of computer that has sent the packet, or name of Windows application that is going to receive the packet, etc.
- **Action** (or verdict) is an instruction to the firewall what to do if the network packet satisfies the Condition of the rule. For example, the firewall can reject the packet if Condition of the rule dictates to drop all the packets for a particular Windows application.

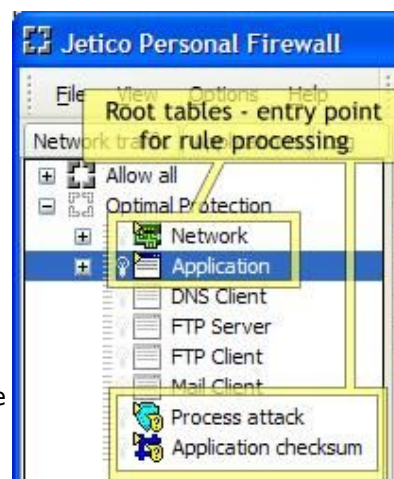


Rule processing order

Entry point for rule processing is the root table of the active Security policy. See [Configuration explorer](#) chapter for more information on Security policy navigating.

Jetico Personal Firewall picks rules from current table in series and tests network event parameters against rule condition. The current table processing lasts until one of the following happens:

- a suitable rule is found and 'Action' field of the rule is **accept** or **reject**. The firewall stops rule processing and takes corresponding action .
- a suitable rule is found and 'Action' field of the rule is **go to table**. In this case the firewall continues the process of the network packet analysis, but instead of choosing next rule from the current table, the firewall picks the first rule from table referred to.
- a suitable rule is found and 'Action' field of the rule is **ask user**. Jetico Personal Firewall displays a [Popup message](#) and waits for user's decision. Further processing depends on user's response.
- a suitable rule is not found in the current table and the firewall selects so-called **default rule**, the last rule in the current table. Default rule's action is applied unconditionally. Actions available to default rules are limited to **accept**, **reject** and **continue**.




Please note the **continue** action effect for the default rule. In this case the firewall passes the network event for further processing to the table that is parent for the current table. As it is shown on the picture above, rules in the parent table are iterated starting from the next rule after the one where the firewall earlier dived into the current table.

Rule actions summary

The following table sums up all the possible values for the Jetico Personal Firewall rule actions:

- ✓ **accept** event is passed to the system as if there was no firewall intervention performed.
- ✗ **reject** event is blocked and error is reported to the system.
- ➡ **go to table** pass event to the first rule of another table for further processing.
- ⏪ **continue** no action is performed, event is passed to the next rule; when applied to default rule, 'continue' acts as like 'return': the next rule is the

rule following the one caused transition to current table

 **ask user** inform user about event and wait for user's reply. User will be able to select one of actions above.

Individual types of rules may restrict the set of possible Action values to smaller subset. For example, IP rules do not support 'ask user' Action.

Related info:

[Configuration explorer](#)

Firewall configuration guidelines

Group similar rules together

Grouping similar rules will make your configuration more readable.

It would be even better if you put similar rules into separate table. A set of rules grouped into tables is easier to manage.

Rule order matters

Rule order plays significant role in Jetico Personal Firewall configuration.

Following example shows the importance of rule order.

Rule order	Effective result
Allow any event Deny any event	✔ Allow all
Deny any event Allow any event	✘ Deny all

Default action matters

First, remember that the default action of configuration table is unconditional. All events passed to some table and had not matched one fall into default processing.

Default action set to **Continue** ⬇ means that event reached this point will be returned back to originating table.

Root table notes

The root table of security policy is the only table which accepts rules of any type (Application, Network and Process attack).

Rules of different types control different events. For example application-level rule will never match any of network packets. They just live in parallel worlds.

Please note also that [Configuration explorer](#) does not show the full set of rule parameters for the root table.

Related info:

[Firewall rules processing](#)

Network protocol rule

Network protocol rule is a simple rule capable of filtering network packets on per-protocol basis.

Common parameters

- **Rule name** - human readable rule description
- **Action** - action to be taken on event if rule will match
- **Log level** - event logging level

Protocol module specific parameters

- **Event** - select whether to match incoming packets, or outgoing packets or both
- **Protocol** - known network protocol or protocol number. See [IANA Ethertypes](#) for details.
- **Source/destination address** - 6-byte ethernet address in the **XX:XX:XX:XX:XX:XX** form
- **Stateful inspection** - Stateful inspection (ARP protocol only)
- **ARP opcode** - ARP protocol opcode
- **ARP source IP** - ARP protocol source IP address
- **ARP destination IP** - ARP protocol destination IP address



IP rule

IP filtering module controls network activity at low system level. IP filtering module deals with IP packets only.

Some rule parameters depend on other parameters values. If forbidden combination of parameters will be entered, rule editor will recover and **Rule body** field will display correct condition.

Following set of parameters are available for rule creation.

Common parameters

- **Rule name** - human readable rule description
- **Action** - action to be taken on event if rule will match
- **Log level** - event logging level

General IP packet parameters

- **Event** - select whether to match incoming packets, or outgoing packets or both
- **Protocol** - higher level network protocol. User can either select known protocol or enter [IANA protocol number](#).
- **Partial packet (fragment)** - checks if IP packet is fragmented.
- **TTL** - IP packet's [Time To Live](#) parameter
- **Checksum** - IP packet checksum validity

Address parameters

IP filtering module operates with **Source** and **Destination** IP addresses.

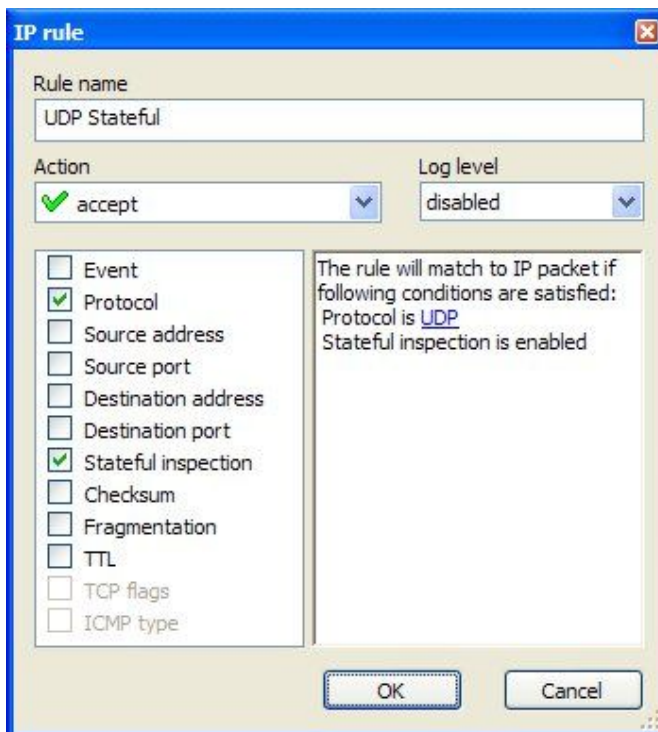
User can specify either

- IP address range in **x.x.x.x-x.x.x.x** form or
- IP address **group** (firewall variable)

Protocol specific parameters

These parameters are available only if **Protocol** is set to either **TCP**, **UDP** or **ICMP**.

- **Source/destination ports** (TCP and UDP only) - allows user to specify ports or port ranges.
- **Stateful inspection** (TCP and UDP only) - match if packet belongs to authorized network communication. Jetico Personal Firewall analyzes TCP and UDP communications' state and discerns expected and out-of-sequence packets.
- **TCP flags** (TCP only) - TCP protocol flags showing TCP connection status. Entire set of flags is controllable (FIN, SYN, RST, PSH, ACK, URG, ECE, CWR)
- **ICMP type/code** (ICMP only) - ICMP protocol code, e.g. well-known Echo and supplemental code /ul>



Application rule

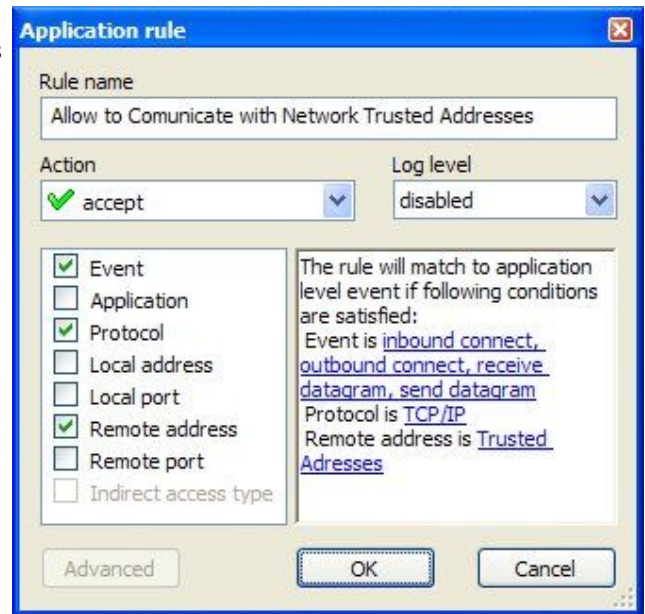
Application filtering rule is intended to control access to network at application level. Following set of parameters are available for application rules.

Common parameters

- **Description** - human readable rule description
- **Verdict** - action to be taken on event if rule will match
- **Log level** - event logging level

Application module specific parameters

- **Application** - full path to application initiated an event. If this field is empty, application is not checked. Both **path** with * and ? wildcards and application **groups** are allowed.
- **Event** - application network event type:
 - **inbound connection** - connection with local application initiated by remote end
 - **outbound connection** - connection to remote server initiated by local application
 - **listening port** - local application waits for incoming connections
 - **receive datagrams** - local application receives data within connectionless communications
 - **send datagrams** - local application sends data within connectionless communications
 - **listening datagrams** - local application waits for incoming data within connectionless communications
 - **access to network** - special event which means general access to networking subsystem preceding to all network communications. While 'access to network' is not enabled for an application, it won't be permitted to execute any network-related function
 - **indirect access to network** - application does not access networking subsystem directly; it forces another application to do all network-related job instead
- **Protocol** - network protocol used for communications. Known protocols include TCP/IP, IPX, local sockets, Appletalk, DECnet, etc.
- **Indirect access type** - type of indirect access to network
 - **inject dll** - application injected dll into networked application's address space
 - **create remote thread** - application created thread on behalf of networking application
 - **write to other's memory** - application wrote into networked application's memory
 - **inter-process call** - application performed inter-process call to networked application
 - **parent process** - application started networked application



Address and port parameters

Address and port parameters are available only if **Protocol** is set to **TCP/IP**.

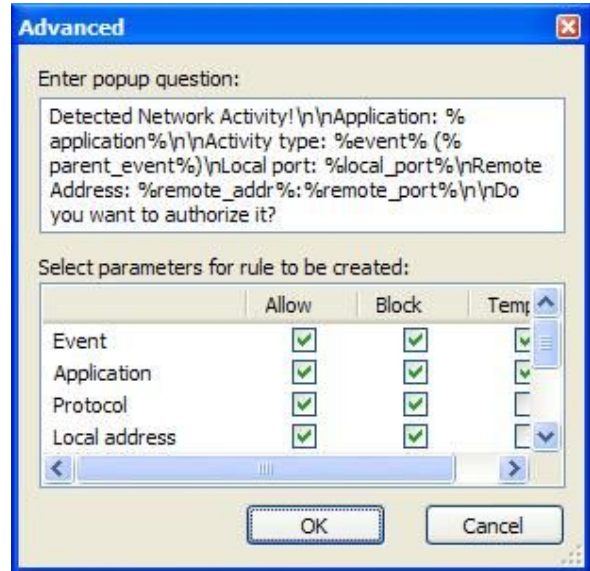
Application filtering module operates with **Local** and **Remote** addresses and ports of network connection.

- **Local/remote address** - User can specify either
 - IP address range in **x.x.x.x -x.x.x.x** form or
 - IP address **group** (firewall variable)
- **Local/remote port** - port range

Advanced options dialog

Advanced options control popup message parameters. **Advanced** button will be enabled if rule action is set to **ask**.

- **popup question** - question text displayed in popup dialog if the rule matches. Text can include keywords in **%keyword%** form. Upon display keywords will be replaced by corresponding values if available. Supported keywords:
 - **event** - event type
 - **application** - path to application executable file
 - **protocol** - protocol
 - **local_addr, remote_addr** - local and remote address
 - **local_port, remote_port** - local and remote ports
 - **parent_event** - event that initiated the activity. For example, parent_event for outbound connection's 'send' and 'receive' event will be 'outbound connection'
 - **misc** - process ID, connection ID
- **parameters for rule to be created** - selected parameters will be checked in the new rule created by popup message if available.



Process attack rule

Process attack rule is designed to filter out following common used hacker's practices

- Running hidden web browser
- Application code modification
- Injecting malicious code to running applications
- Installing global hooks

Common parameters

- **Rule name** - human readable rule description
- **Action** - action to be taken on event if rule will match
- **Log level** - event logging level

Process attack specific parameters

- **Event** - suspicious action type



- **install global hook**

Microsoft Windows operating systems provide so-called hooking mechanism. Application are allowed to install 'hook' function which can intercept some events (mouse actions, keystrokes, etc.) before they reach the target application.

The key point of some hooks is that hook function code must be executed on behalf of other application.

Windows hooking mechanism is widely used both by legal applications and trojans. As soon as trojan installs Windows hook, it can access network via its hook function. Since the hook function can reside in legal process' space (for example, in Explorer.exe process), the user will not realize that network is accessed by the trojan.

- **create hidden window**

Trojan program can run another trusted application with command-line arguments and make the application accessing network. Of course, the user will notice that something is going wrong if he/she sees unexpectedly appeared Internet Explorer's windows. So the trojan program can simply run Internet Explorer's windows in hidden mode.

Jetico Personal Firewall reports about the event, but it should be noted that legal programs often run their modules with hidden windows, for example, when such a module supports icon in the system tray.

- **write to application's memory**

Trojan program can modify memory of another trusted application. Usually trojan replaces contents of memory where legal code of the trusted application resides by the code of the trojan's procedure that accesses network. As soon as the procedure runs, it accesses network so that everything looks like the trusted application itself decides to access network.

- **create remote thread**

When Windows application runs, it may have one or several so-called "threads". Every thread works in parallel with other threads and executes its own code in the context of the application's process.

Windows allows creating of remote threads, i.e. one process can create thread that will work in context of another trusted process. In this case Windows believes that this trusted process is responsible for everything that the remote thread makes.

Trojan programs can use the technology of remote threads to hide their activity.

- **modify child process**

Trojan program (attacker) can run another trusted application and modify its memory before the process of trusted application will run. Since the trusted process is not running yet, it may be difficult to detect after some time that the trusted application will run the code of trojan program.

- **direct memory access**

Trojan program can harm loaded Windows system modules or running applications by modifying contents of system physical memory. Since the physical memory is common for all the processes running on the computer, such a dangerous program can make any process doing what the trojan program wants. Windows security mechanisms normally does not allow

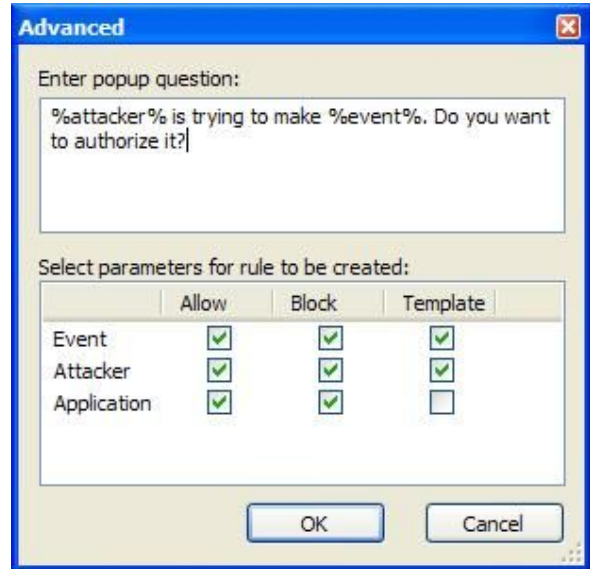
programs to make such a trick, but it is still possible. If Jetico Personal Firewall detects this kind of attack, it definitely means that the reported program is a trojan.

- **Attacker** - application performing suspicious activity. Both **path** with * and ? wildcards and application **groups** are allowed.
- **Application** - application suffering from attack. Both **path** with * and ? wildcards and application **groups** are allowed.
Some attacks, such as hook installing, affect many applications. In that case Victim values becomes useless

Advanced options dialog

Advanced options control popup message parameters. **Advanced** button will be enabled if rule action is set to **ask**.

- **popup question** - question text displayed in popup dialog if the rule matches. Text can include keywords in **%keyword%** form. Upon display keywords will be replaced by corresponding values if available. Supported keywords:
 - **event** - event type
 - **application** - path to application executable file
 - **attacker** - path to attacker application executable file
 - **misc** - additional information
- **parameters for rule to be created** - selected parameters will be checked in the new rule created by popup message if available.



Hash checking rule

Hash checking layer is a supplement to Process attack and Application layers. All Process attack and Application events are passed to Hash checking filter first.

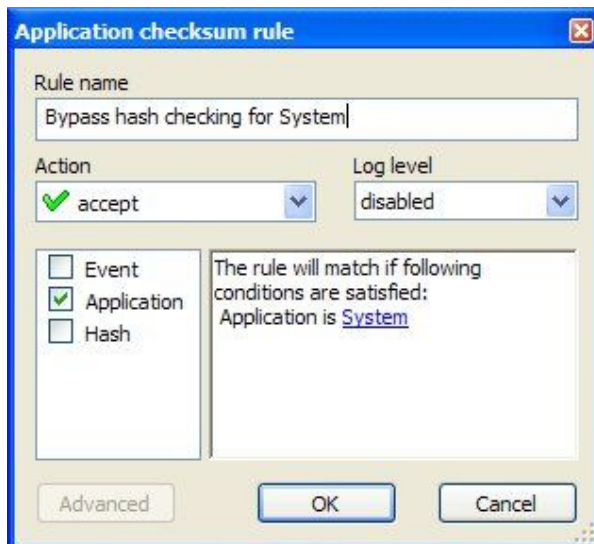
Common parameters

- **Rule name** - human readable rule description
- **Action** - action to be taken on event if rule will match
- **Log level** - event logging level

Hash checking specific parameters

- **Event** - event type
 - **access to network**
application level "access to network" event
 - **indirect access**
Application level "indirect access to network" event
 - **network activity**
All other application and process attack events.

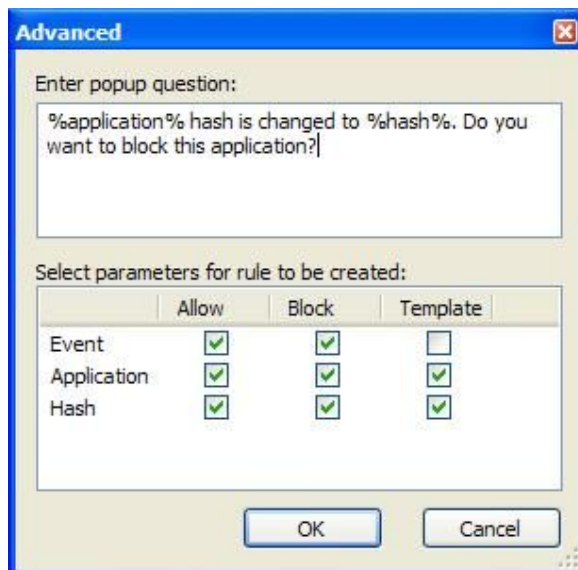
- **Application** - full path to application initiated an event. If this field is empty, application is not checked. Both **path** with * and ? wildcards and application **groups** are allowed.



Advanced options dialog

Advanced options control popup message parameters. **Advanced** button will be enabled if rule action is set to **ask**.

- **popup question** - question text displayed in popup dialog if the rule matches. Text can include keywords in **%keyword%** form. Upon display keywords will be replaced by corresponding values if available. Supported keywords:
 - **event** - event type
 - **application** - path to application executable file
 - **hash** - application file SHA-1 hash
 - **misc** - additional information
- **parameters for rule to be created** - selected parameters will be checked in the new rule created by popup message if available.



Creating new rule

To create new firewall rule do following actions:

1. Select [Configuration explorer](#) tab.
2. Select desired target table in the Configuration explorer's left pane.
3. Proceed to Configuration explorer's right pane - table view.
4. Press **Insert** or call table view's context menu by clicking Right Mouse Button, then select **New... >** menu item.
5. Use arrows **↑** **↓** or mouse to select rule type.
6. Rule editing dialog will be brought up to you. Please edit and press **OK**

Related info:

[Configuration explorer](#)

Rule editing

To edit firewall rule do following actions:

1. Select [Configuration explorer](#) tab.
2. Select desired target table in the Configuration explorer's left pane.
3. Select Configuration explorer's left pane - table view.
4. Select rule to edit
5. Double-click on selected rule or press **Enter** or call table view's context menu by clicking Right Mouse Button, then select **Edit** menu item.
6. Rule editing dialog will be brought up to you. Please edit and press **OK** to accept or **Cancel** to decline changes.

Related info:

[Configuration explorer](#)

Enabling and disabling rules

To change rule state do following actions:


1. Select [Configuration explorer](#) tab.
2. Select desired target table in the Configuration explorer's left pane.
3. Checkbox at "Action" column indicates curent rule state.
 - Rule is enabled.
 - Rule is disabled.
 - The state of table's default action is always **Enabled** and could not be changed.
 - An error occured during rule loading. Hence rule was not loaded and has no effect.
4. Click checkbox to change rule state.
5. Please note that multiple rule selection is allowed.

Related info:

[Configuration explorer legend](#)

Deleting rules

To delete firewall rule do following actions:

1. Select [Configuration explorer](#) tab.
2. Select desired target table in the Configuration explorer's left pane.
3. Select rule to delete in the Configuration explorer's right pane. Note that multiple selection is allowed.
4. Remember that the last rule of table represents table's default action and could not be removed.
5. Press **Delete** or call table view's context menu by clicking Right Mouse Button, then select  menu item.



Related info:


[Configuration explorer](#)

[Enabling and disabling rules](#)

Copying and moving rules

Both copying and moving rules require similar actions:

1. Select [Configuration explorer](#) tab.
2. Select desired target table in the Configuration explorer's left pane.
3. Select Configuration explorer's left pane - table view.
4. Select and drag rule to its new position. Note that multiple selection is allowed. Use
 - **Right Mouse Button** for copying rules. Mouse pointer  indicates rule copying mode.
 - **Left Mouse Button** for copying rules. Mouse pointer  indicates rule moving mode.



The thick black line shows rule insertion position. Prohibitive  mouse pointer indicates that current target is not acceptable for copying or moving the rule.


5. If you need to copy or move the rule between tables simply point at target table in Configuration explorer while dragging.
6. Drop the rule to desired location.
7. If you copy/move multiple rules, they will be gathered together with original order preserved.

Please note that rule order is significant part of firewall configuration. Reordering rules may impact your system protection. Do it carefully.

Copying and moving tables

Both table copying and moving require similar actions:

1. Select [Configuration explorer](#) tab.
2. Select and drag desired table to its new position in the Configuration explorer left pane . Use
 - **Right Mouse Button** for copying rules. Mouse pointer  indicates copying mode.
 - **Left Mouse Button** for copying rules. Mouse pointer  indicates moving mode.

Prohibitive  mouse pointer indicates that current target is not acceptable for copying or moving the table.

3. Drop the table to desired location.

Creating template for Popup message

Template internals

Whenever you choose 'Use template:' option in the [Popup message](#) and press new firewall rule is added to configuration.

The rule will have the action '[Go to another table](#)' with target table you have just chosen.

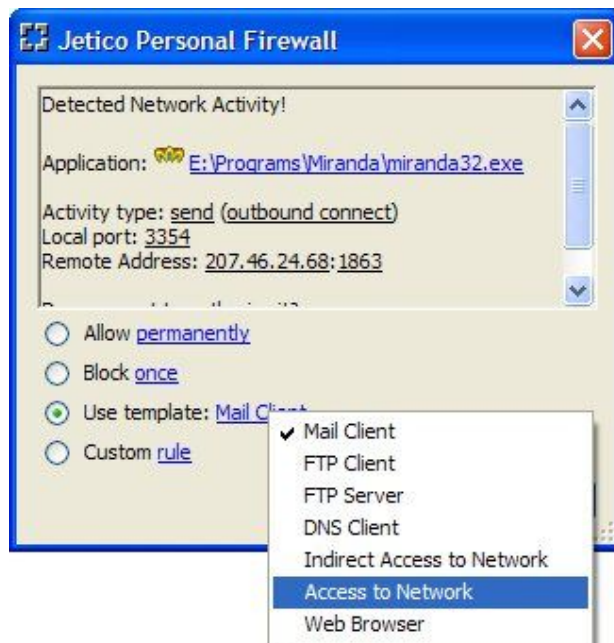
Thus in order to populate 'Use template:' list you should create special template table.

Template table criteria

For a particular rule 'Use template:' list contains all tables allowed to refer to.

The condition above could be translated to following criteria:

1. Template table must be of same type as the originating rule.
2. Template table must not refer, directly or indirectly to the table containing the originating rule.



Related info:

[Configuration explorer](#)

Glossary

Cracker

a person who tries to get unauthorized access to computer.

Denial of Service

a type of remote attack which disrupts normal work of target.

Firewall

software (or hardware) system intended to protect computers from network attacks.

Gateway

a system which forwards network packets.

ICMP

an auxiliary protocol for service and control messages, member of TCP/IP family.

IP

a protocol for network packets level in TCP/IP family.

ISP, Internet Service Provider

someone who provides Internet access to you.

Network

a set of interconnected computers which are able to pass information to each other.

Packet

an atomic piece of information passed via network.

Stateful inspection

network packet processing aware of connection state.

TCP

a protocol for reliable data transfer, member of TCP/IP family.

Trojan Horse or Trojan

a camouflaged malicious program which hides its true purpose.

TTL (Time To Live)

a field in the IP protocol that specifies how many more hops(routers) a packet can travel before being discarded or returned.

End-user license agreement

JETICO PERSONAL FIREWALL - PRODUCT LICENSE INFORMATION

NOTICE TO USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT. USE OF THE JETICO PERSONAL FIREWALL SOFTWARE PROVIDED WITH THIS AGREEMENT (THE "SOFTWARE") CONSTITUTES YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THIS SOFTWARE. USER'S USE OF THIS SOFTWARE IS CONDITIONED UPON COMPLIANCE BY USER WITH THE TERMS OF THIS AGREEMENT.

1. LICENSE GRANT. Jetico, Inc. grants you a license to use the freeware version of this SOFTWARE. "Use" means storing, loading, installing, executing or displaying the SOFTWARE.
2. OWNERSHIP. The SOFTWARE is owned and copyrighted by Jetico, Inc. Your license confers no title or ownership in the SOFTWARE and should not be construed as a sale of any right in the SOFTWARE .
3. COPYRIGHT. The SOFTWARE is protected by copyright law of Finland and international treaty provisions. You acknowledge that no title to the intellectual property in the SOFTWARE is transferred to you. You further acknowledge that title and full ownership rights to the SOFTWARE will remain the exclusive property of Jetico, Inc and you will not acquire any rights to the SOFTWARE except as expressly set forth in this license. You agree that any copies of the SOFTWARE will contain the same proprietary notices which appear on and in the SOFTWARE.
4. REVERSE ENGINEERING. You agree that you will not attempt to reverse compile, modify, translate, or disassemble the SOFTWARE in whole or in part.
5. NO OTHER WARRANTIES. JETICO, INC DOES NOT WARRANT THAT THE SOFTWARE IS ERROR FREE. JETICO, INC DISCLAIMS ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.
6. SEVERABILITY. In the event of invalidity of any provision of this license, the parties agree that such invalidity shall not affect the validity of the remaining portions of this license.
7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL JETICO, INC OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE DELIVERY, PERFORMANCE OR USE OF THE SOFTWARE, EVEN IF JETICO, INC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL JETICO, INC' LIABILITY FOR ANY CLAIM, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, EXCEED THE LICENSE FEE PAID BY YOU, IF ANY.
8. GOVERNING LAW. This license will be governed by the laws of Finland as they are applied to agreements between Finland residents entered into and to be performed entirely within Finland. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.
9. ENTIRE AGREEMENT. This is the entire agreement between you and Jetico, Inc which supersedes any prior agreement or understanding, whether written or oral, relating to the subject matter of this license.

©Jetico, Inc.

Technical support

If you have any suggestions or comments on making the Jetico Personal Firewall or this documentation better, contact us via

E-mail: support@jetico.com

supplying your name and Internet address..

We invite you to make the acquaintance of our WWW -site to get the recent information on our products and others:

<http://www.jetico.com>

Note that your comments become the property of Jetico, Inc.

Thank you for your time!

Jetico Team