Table of Contents

Getting started with Irbis Firewall

Irbis Firewall is a Firewall application for Microsoft Windows ME/2000/XP developed to protect your computer from network attacks while it is connected to the network. This part describes most common actions you can perform with Irbis Firewall.

Irbis Firewall Startup

Irbis Firewall is ready to work immediately after the installation complete. To run Irbis Firewall, push the **Start** button, select the **Programs** submenu, then move into the **Irbis Firewall Enterprise Suite** submenu and click **Irbis Firewall**. The first run of the Irbis Firewall uses default settings which are enough to protect a standalone PC connected to the Internet.

If you wish Irbis Firewall to run automatically after your computer boots up, use the Startup panel in the Irbis Firewall configuration dialog accessed through the System menu.

Changing security level

If you wish to change the security level provided by Irbis Firewall, use the Security panel in the Irbis Firewall configuration dialog accessed through the System menu.

This following table shows what security level may be used for some of the typical situations:

Highest security level	Computers used for limited network tasks like browsing WWW, using ICQ, reading e-mail, etc.
High security level (default)	Recommended for most users. Allows working with arbitrary number of network services (WWW, ICQ, FTP, e-mail, TELNET, SSH, etc), except on-line games.
Medium security level	Computers used for unlimited work in network, including on-line FPS and RTS (first-place shooter and real-time strategy) games.
Low security level	Protects only basic Windows subsystems without any other limitations.

Embedded proxy server startup

Irbis Firewall has an embedded HTTP proxy server allowing you to share single Internet connection with a group of computers without insecure Windows Internet Connection Sharing. The default configuration disables the embedded proxy server. To enable it, use the Proxy server parameters panel in the HTTP proxy server configuration dialog window accessed through the System menu. After enabling the embedded HTTP proxy server don't forget to change the settings of your browser and download programs properly.

View Irbis Firewall logs

To view Irbis Firewall log files, use the Irbis Firewall Log Window accessed through the Log Files menu. You can also use the **Irbis Firewall Log Viewer** application, which is in the same **Programs** submenu as Irbis Firewall.

Changing interface language

To change the Irbis Firewall interface language, select the **Change language** item in the System menu. After you select a new language, all Irbis Firewall messages and captions will display in the selected language.

Creating your own configuration

To create a non-standard configuration use the Irbis Firewall Configuration Dialog. Select the Security panel, then select **Custom settings**, and click **Customize**. Create the rulesets with rules and policy you need, using the Irbis Firewall Manual Configuration Dialog. Then select the Bindings panel and set associations between the IP-addresses of interfaces and your rulesets. When you are done click **OK** to save the changes and check the result.

Irbis Firewall Overview

Irbis Firewall is a firewall application developed for using on Microsoft Windows 2000, Windows XP and Windows ME operating systems. The primary function of Irbis Firewall is the filtration of the IP-packets based on the network-level fields of packets, such as source and destination addresses, source and destination ports, ICMP messages types and codes. Irbis Firewall doesn't filter packets on the application-level for not to decrease Windows functioning safety by installing necessary drivers.

Irbis Firewall distributive package contains four programs:

- Irbis Firewall filter and management application (Irbis.exe), which allows you to configure Irbis Firewall easily and monitor its work. This application can also work as a packet filter if service application is not active.
- The service application (IrbisSVC.exe), which works in the service (background) mode when the **Service mode** is on.
- Irbis Firewall Log Export application (LogExport.exe) for exporting Irbis Firewall log files from the internal format to text files
- Irbis Firewall Log Viewer (LogMon.exe), which allows monitoring Irbis Firewall log files without running the control application.

After startup Irbis Firewall automatically starts the process of packet filtration. The filtration is applied to all the packets sent or received through any IP-interface. Irbis Firewall also tracks activation and deactivation of interfaces, and applies separate filtering rules to each active interface. This technology makes Irbis Firewall protection very flexible and allows you to customize the network activity of your computer.

Binding is a process which associates input and output filtering rulesets with an active IP-interface. While binding rulesets to interfaces, Irbis Firewall uses the **binding table**, which defines rulesets applied to the IP-interface. Binding table is created automatically if you use one of the standard security levels selected on the Security panel of the Configuration Dialog. If you use your own configuration, you can define your own binding table.

The required binding is selected according to the following principles: bindings are searched in order of increasing the net size defined by the **Network mask** value, i.e. bindings for a smaller subnet are of more priority. If required binding is not found in the table, the **default binding** is used.

Filters (also called **Rulesets**) are sets of rules (see Rulesets Configuration Panel for details). These sets describe the packets that should be accepted or rejected. While creating rules, you may use **Areas** (areas are sets of IP-addresses, see Areas Configuration for details). Areas allow you to group any set of hosts so you can use them as single addresses.

Irbis Firewall also supports special addresses. These addresses are evaluated only when a ruleset that contains such special address is bound to IP-interface. Here is a list of such addresses:

- **local** - IP-address of interface itself
- **local net** - IP-address of subnet that interface belongs to
- **subnet broadcast** - broadcast address of network that interface belongs to
- **nameservers** - all DNS servers
- **broadcast** - all broadcast address 255.255.255.255
- **any** - any IP-address (0.0.0.0/0.0.0.0)

The last two special addresses always have the same value, and were designed to improve IPv6 support in future releases.

Additional capabilities

Irbis Firewall has an embedded HTTP proxy server. This server is not enabled default, so you have to use the Configuration Dialog to enable it. A proxy server supports CONNECT, GET, HEAD and POST methods, and allows you to control access with the following conditions:

- Client computer IP-address
- Server address
- Part of server address
- Requested document name
- Part of requested document name
- Request method

Irbis Firewall HTTP Proxy Server Overview

Common Information

- Client interaction via **HTTP** protocol version **0.99**, **1.0** and **1.1**
- Support of document requests via **HTTP** and **FTP** protocols
- Access control based on the following criteria:
  - Client IP-address
  - Server name
  - Document name
  - Server name substring
  - Document name substring
  - Request type
- Arbitrary combinations of all criteria realized

Irbis Firewall embedded proxy server uses access control lists and access control expressions.

Access control lists are virtually named conditions. This means that any access control list is a condition, and it should have a unique name. Each request may satisfy or not satisfy to a single access control list. E.g. if an access list is based on a client IP address, then a request from the computer with this IP-address is accepted by this access control list, and all other requests are not.

Access control expression is a set of one or more access control lists and an action to perform on request if it is accepted by each of these lists. Each access control list in the expression may have an inversion flag. The expression becomes true if the request is accepted by all the lists, which have no inversion flags set, or if the request is not accepted by all the lists, which have the inversion flags set.

Take a look at the example:

- **Accounting Department** access control list is a client IP address-based list, and client IP address in this list is set to **192.168.0.0/255.255.255.0**.
- **GIF Files** access control list is a document name substring-based, and a substring document name searched is set to **.gif**.
- Access control expression contains
    - ACL **Accounting department** without inverse flag set
    - ACL **GIF-files** with inverse flag set

The action defined for this access control expression takes place if a request comes from the computer with IP-address from the subnet 192.168.0.0/255.255.255.0 and requested document name does not contain a **.gif** substring.

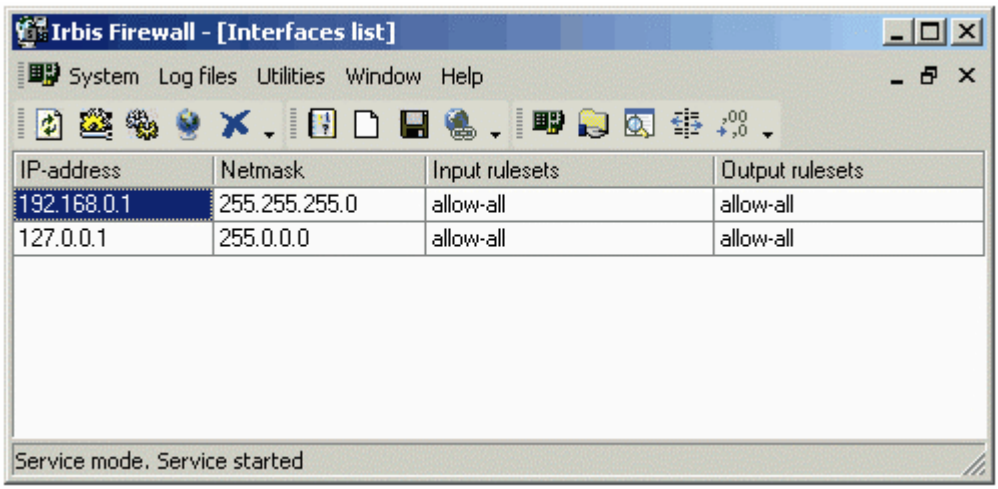
Irbis Firewall proxy server supports three kinds of actions:

- Allow access (Irbis Firewall executes request and sends server reply to the client)
- Deny access (Irbis Firewall notify client that request was cancelled)
- Access through parent (Irbis Firewall sends request to the parent proxy server)

Irbis Firewall Main Window

The picture below shows the main Irbis Firewall window. On closing this window Irbis Firewall does not finish its work. It stays accessible through an icon in the system tray area, which looks like an **i** letter in a green, yellow or red circle (depends on the current Irbis Firewall mode). Click this icon to restore the main Irbis Firewall window, or right-click for the popup menu.

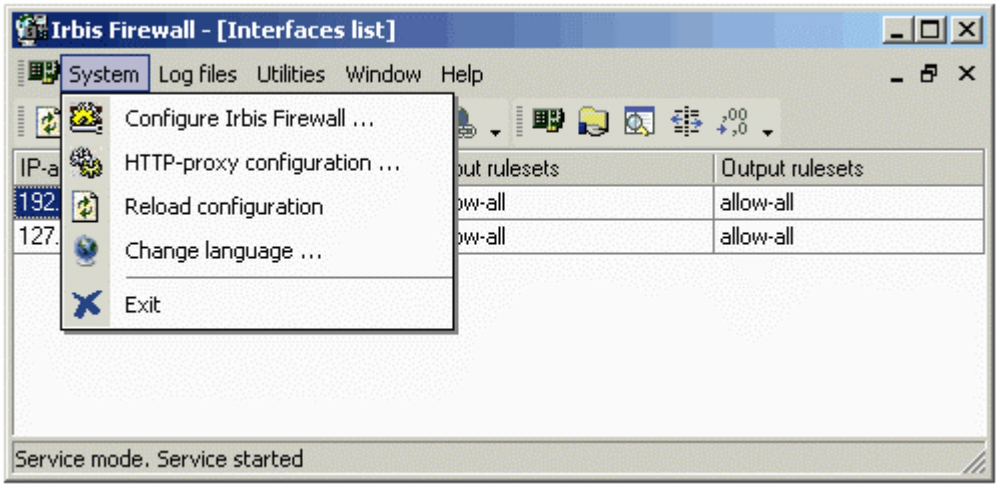
Picture 1. Irbis Firewall main window



Picture 2. System tray area icon

System Menu

The **System** menu allows you to customize the system settings of Irbis Firewall, such as security level, startup and work mode, HTTP proxy configuration, interface language, and more.



Configure Irbis Firewall...
Shows the Irbis Firewall Configuration Dialog for customizing Irbis Firewall system settings.

HTTP-proxy configuration...
Shows the Irbis Firewall Embedded Proxy Server Configuration Dialog.

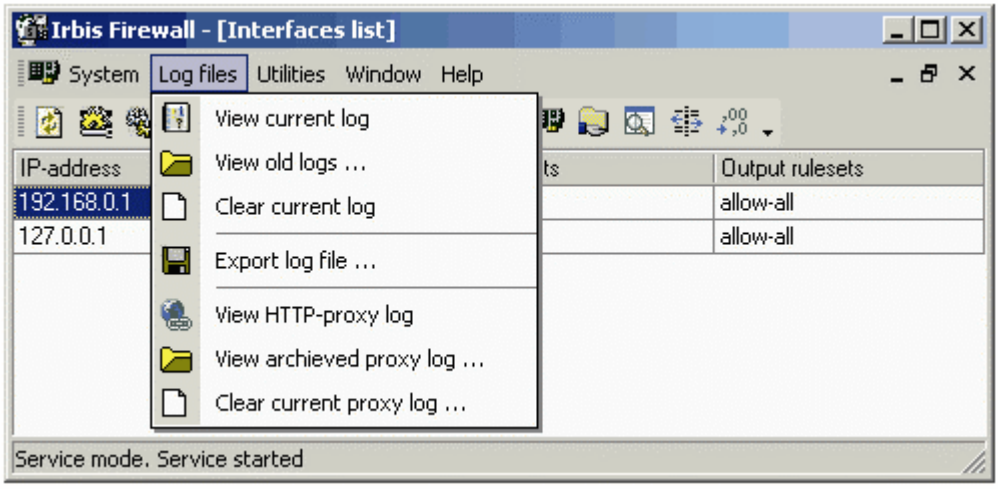
Reload configuration
Reloads Irbis Firewall configuration.

Change language
Allows you to select the Irbis Firewall interface language

Exit
Closes the main window and exits Irbis Firewall.

Log Files Menu

The **Log files** menu allows you to work with Irbis Firewall log files which contain complete lists of rejected IP-packets.



View current log
Displays the current Irbis Firewall log file. This log file contains a list of all packets rejected by the rulesets after last log file archiving. See Log View Window for details.

View old logs...
This option allows viewing archived (not current) log files. Log files are archived automatically when their size exceeds the configured value.

Clear current log...
Deletes the current log file after confirmation.

Export log file...
Calls the export utility to export a log file from an internal Irbis Firewall log format into a plain text file. See Irbis Firewall Log Export for details.

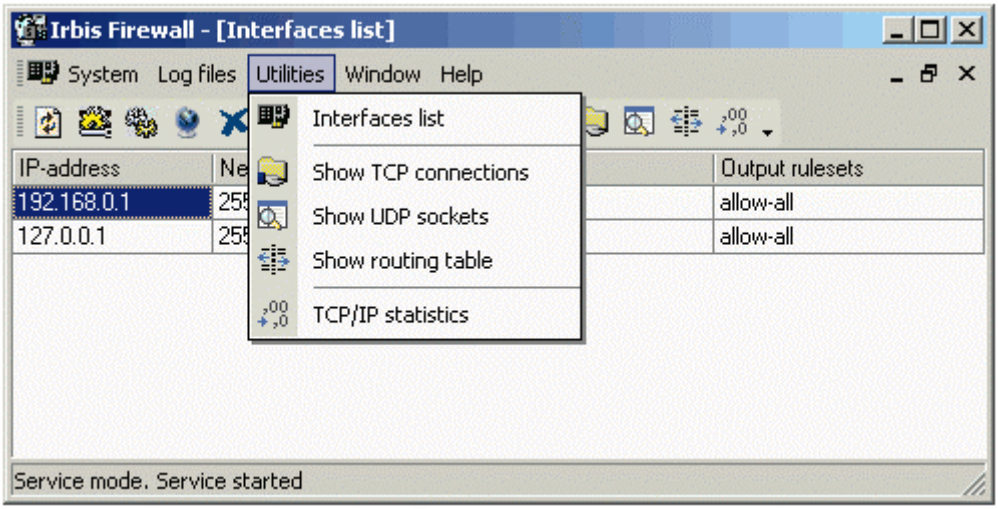
View HTTP-proxy log...
Displays the current HTTP-proxy server log.

View archived proxy log...
Allows viewing archived HTTP-proxy server log.

Clear current proxy log...
Deletes the current HTTP-proxy server log after a confirmation.

Utilities Menu

The **Utilities** menu gives you additional information about the TCP/IP stack on your computer. This statistics can be useful while optimizing your computer network or fixing some network problem.



Interfaces list
Displays the list of active IP-interfaces and the rulesets applied to these interfaces.

Show TCP connections
Displays the list of opened TCP connections, including listening sockets.

Show UDP sockets
Displays the list of opened UDP sockets on your computer.

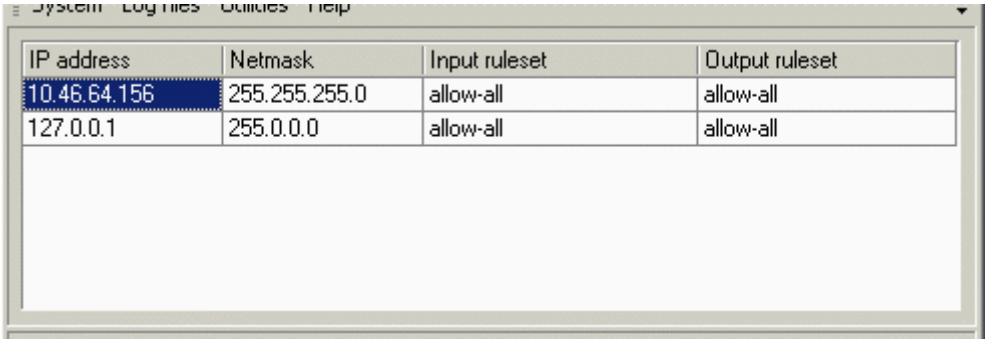
Show routing table
Displays the full routing table of IP packets on your computer.

TCP/IP statistics

Displays the TCP/IP internal counters and statistics.

Interfaces

The Interface list allows you to view the list of all active IP-interfaces on your computer, and the rulesets applied to these interfaces.



IP address
Lists the IP-addresses of active IP-interfaces on your computer.

Netmask
Lists the subnet masks of active IP-interfaces on your computer.

Input ruleset
Lists names of rulesets applied to packets received via the corresponding IP-interfaces.

Output ruleset
Lists names of rulesets applied to packets sent via the corresponding IP-interfaces

Status bar

The Irbis Firewall status bar displays information about the Irbis Firewall working mode. There are two modes: **Standalone** and **Service**. The status bar provides additional info for each mode.

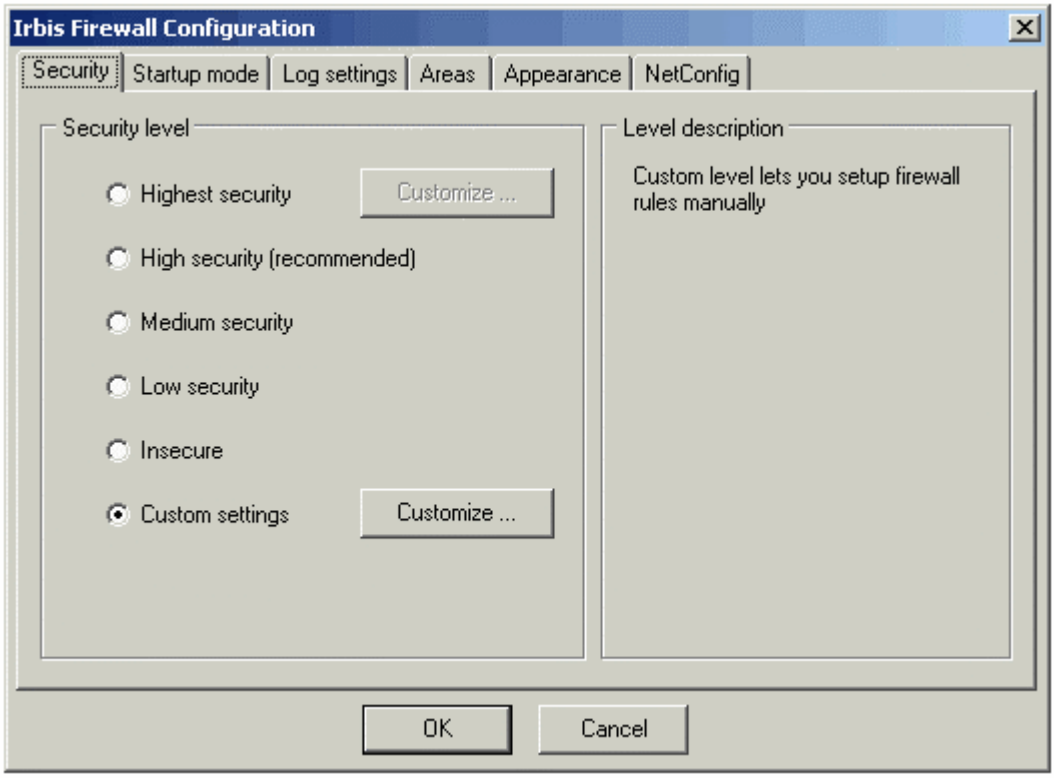
Mode	Service state	Local filters	Status bar text	SysTray icon color
Standalone	N/A	Active	Standalone mode. Filtration started	Green
Service mode	Started	Inactive	Service mode. Service started	Green
Service mode	Stopped	Active	Service mode. Service stopped. Local filtration started	Yellow
Service mode	Stopped	Inactive	Service mode. Service stopped. Filtration not started	Red

Irbis Firewall Configuration Dialog

The Irbis Firewall **Configuration Dialog** has six panels with controls grouped by their functions.

Security

The **Security** panel allows you to select the security level of Irbis Firewall. The panel is divided into two parts: the left part allows you to select the security level, and the right part displays the selected level description.



Irbis Firewall provides you with six security levels:

Highest security
Allows only user-defined services.

High security
Keeps your computer out of actually all network attacks and scans, including but not restricted to CodeRed-style attacks.

Medium security
Protects your computer from the most network attacks, but also grants your computer more freedom to use network services

Low security
Protects only most vulnerable Windows subsystems

Insecure
Switches all security off

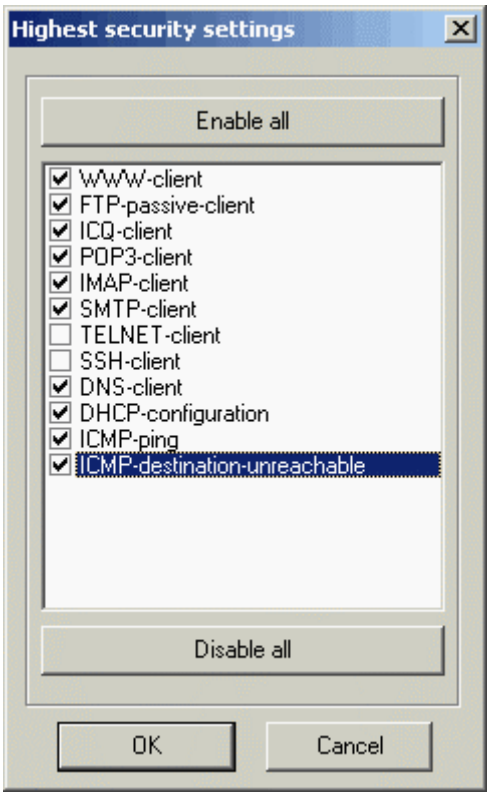
Custom settings
Allows you to define the security rules manually. This can be used by advanced users and system administrators to configure each aspect of IP packet filtration.

Customize ...
These buttons activate the proper dialogs for customizing **Highest** and **Custom Setting** levels.

See Highest Security Level Configuration Dialog and Custom Setting Level Configuration Dialog for details.

Highest Security Level Configuration Dialog

The **Highest Security Level Configuration Dialog** allows you to select the network services available for programs running on your computer.



The list of services allows you enable/disable available services.

Enable all
Enables all services in the list.

Disable all
Disables all services in the list.

Custom Security Level Configuration Dialog

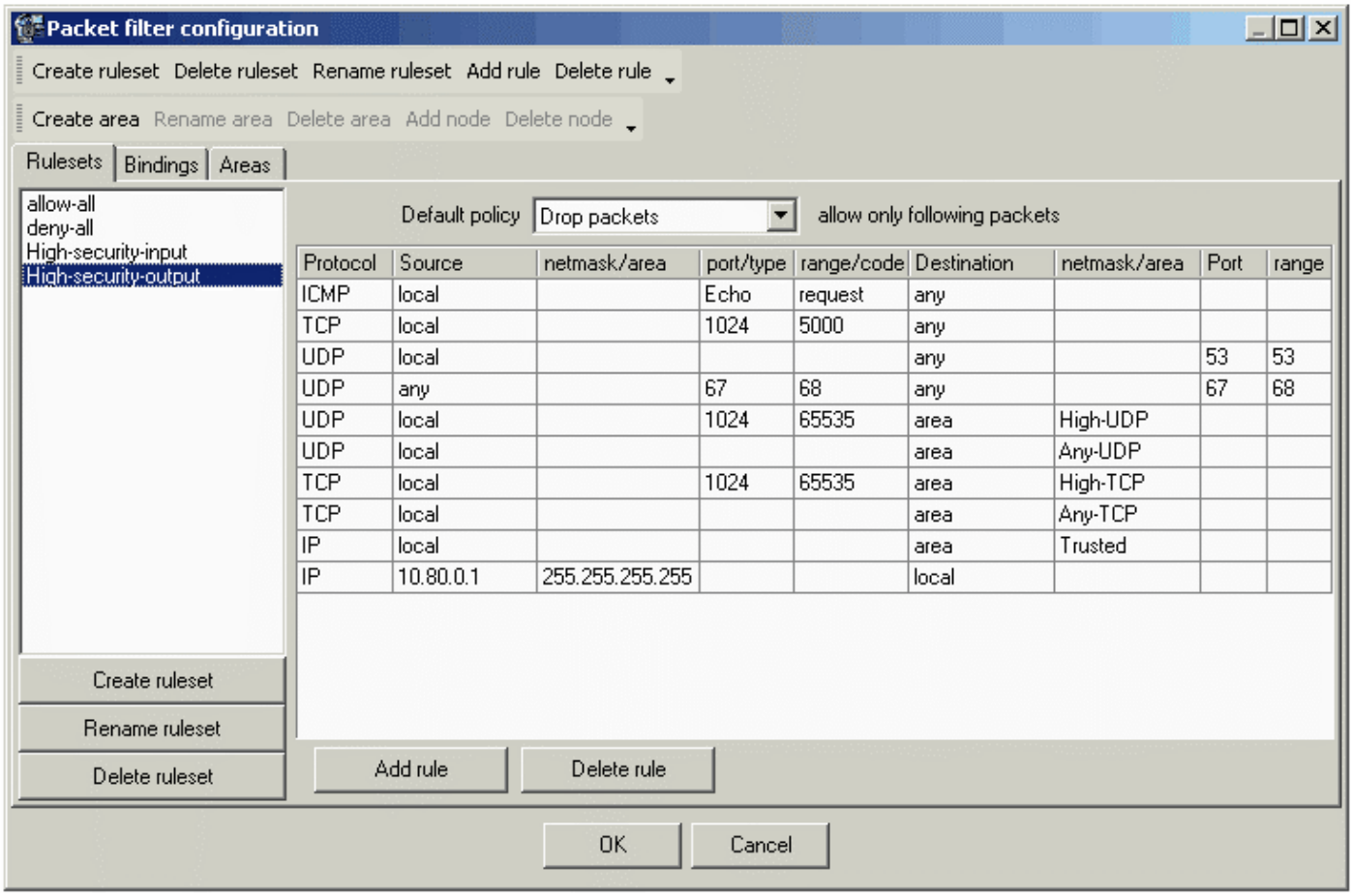
The **Custom Security Level Configuration Dialog** allows you to configure all settings of IP packets filtration manually. This dialog window has three panels:

Rulesets

The **Rulesets Configuration Panel** allows you to manage rulesets that are used for filtering incoming and outgoing IP packets through the IP interfaces on your computer. Each ruleset has a **default policy** and a set of exception rules.

When default policy is **Permit packets**, any packet accepted by any rule is rejected (destroyed), and a packet not accepted by all the rules is allowed to be sent or received. When default policy is **Drop packets**, any

packet accepted by any rule is allowed to be sent or received, and a packet not allowed by all the rules is rejected (destroyed).



Create ruleset
Calls the ruleset creation wizard for creating a new ruleset.

Rename ruleset
Allows you to rename the selected ruleset.

Delete ruleset
Removes the selected ruleset.

Add rule
Adds a new exception rule to the selected ruleset.

Delete rule
Removes the exception rule from the selected ruleset.

Default policy
Allows you to change the default policy for the selected ruleset.

Exception-rule table columns

Protocol
Protocol declared in the packet header.

Source

The IP address of the packet sender. This IP address may be a subnet address, or a special address. There are some kinds of special addresses:

- **local** - your computer IP address;
- **local net** - address of the subnet, to which your computer is connected;
- **any** - any IP address;
- **broadcast** - broadcast address 255.255.255.255;
- **net broadcast** - broadcast address of the subnet, to which your computer is connected;
- **area** - link to the user-defined set of hosts (area). See Areas Configuration Panel for details.

netmask/area
A subnet mask for the sender address, or an area name if area is selected in the **Source** column.

port/type
The lowest number of the sender port number range for the TCP or UDP protocols, or an ICMP message type if the ICMP protocol selected.

port/code
The highest number of the sender port number range for the TCP or UDP protocol, or an ICMP message code if the ICMP protocol is selected.

Destination
IP address of the packet destination. This can be a special address.

netmask/area
Subnet mask for the destination IP address, or an area name if the destination address is an area.

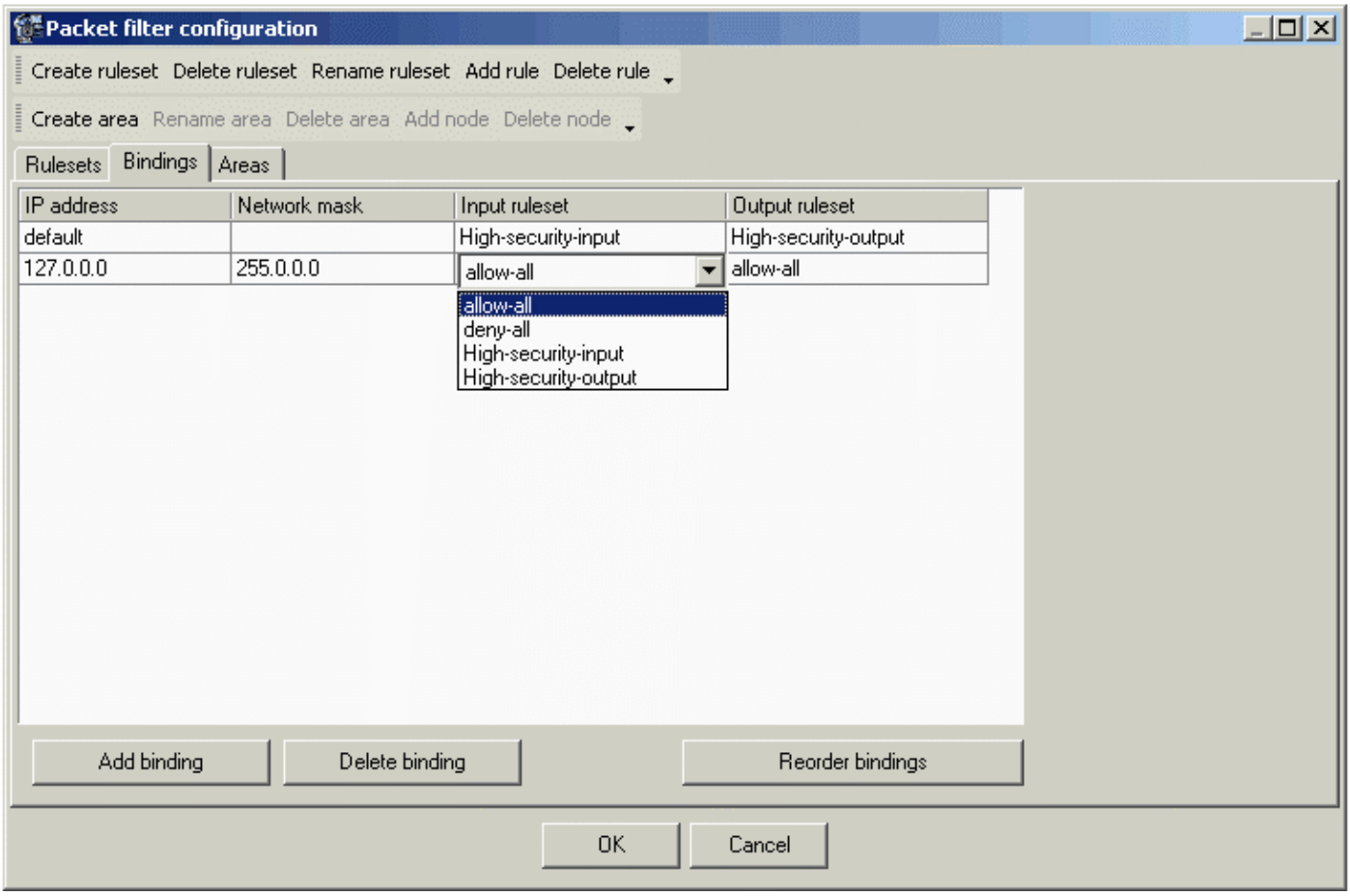
Port
The lowest number of the destination port number range.

range
The highest number of the destination port number range.

Bindings

The **Bindings Configuration Panel** allows you to define conditions used for applying rulesets to IP interfaces. For each IP interface Irbis Firewall selects two rulesets depending on the interface IP address. One ruleset is used to filter the incoming packets; the second one is for the outgoing packets.

For each IP interface Irbis Firewall searches for the row with minimal subnet that contains IP address of this interface. If there is no such row, Irbis Firewall uses the **default** binding. Default binding row cannot be removed, but can be changed so you may be sure that each interface is bound with rulesets.

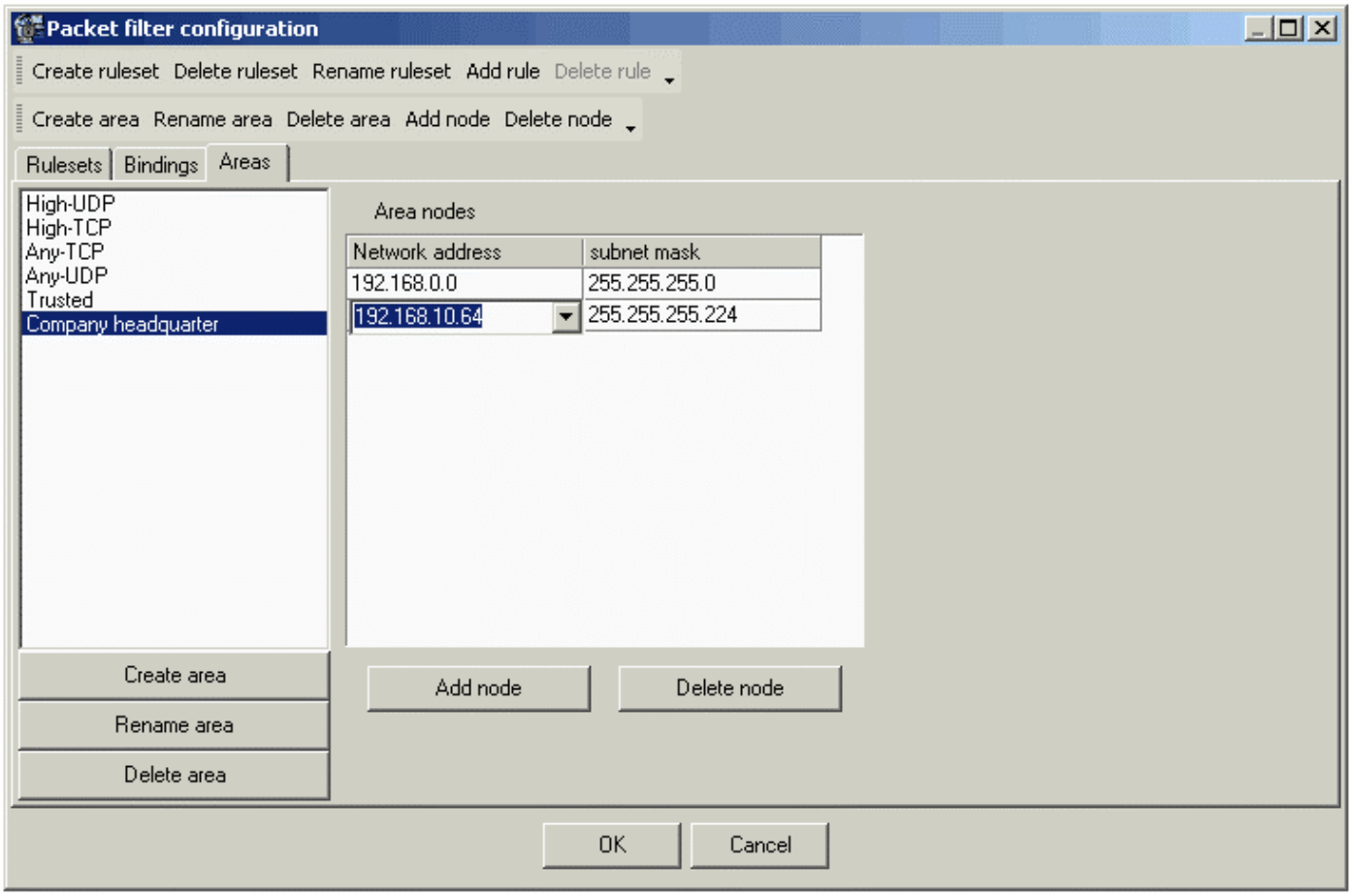


Add binding
Appends a new row to the binding list.

Delete binding
Removes the selected row from the binding list.

Areas

The **Areas Configuration Panel** allows you to manage areas. Areas are very useful objects that greatly improve the process of managing firewall rules. Every area should have a unique name and can have any number of IP addresses and special addresses. Irbis Firewall creates several empty areas default that can be used to allow some computers connect to your computer even in the high secure levels.



Create area
Creates a new area.

Rename area
Allows you to rename the selected area.

Delete area
Removes the selected area.

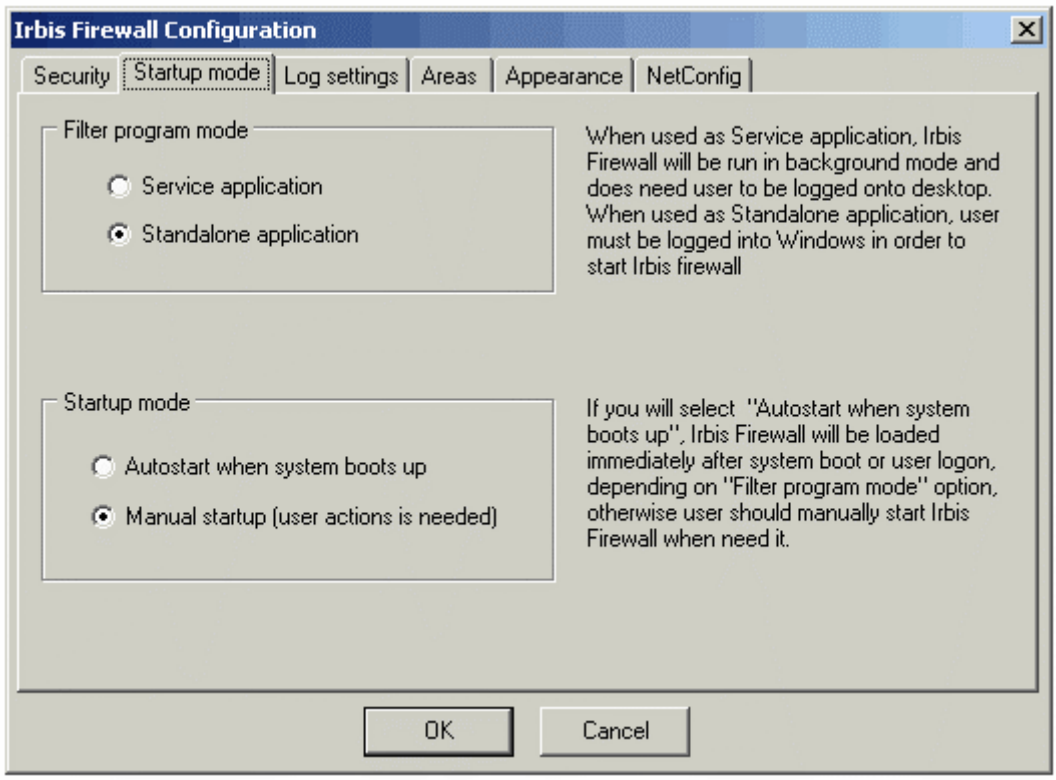
Add node
Adds a new address to the selected area.

Delete node
Removes the selected address.

Startup Mode

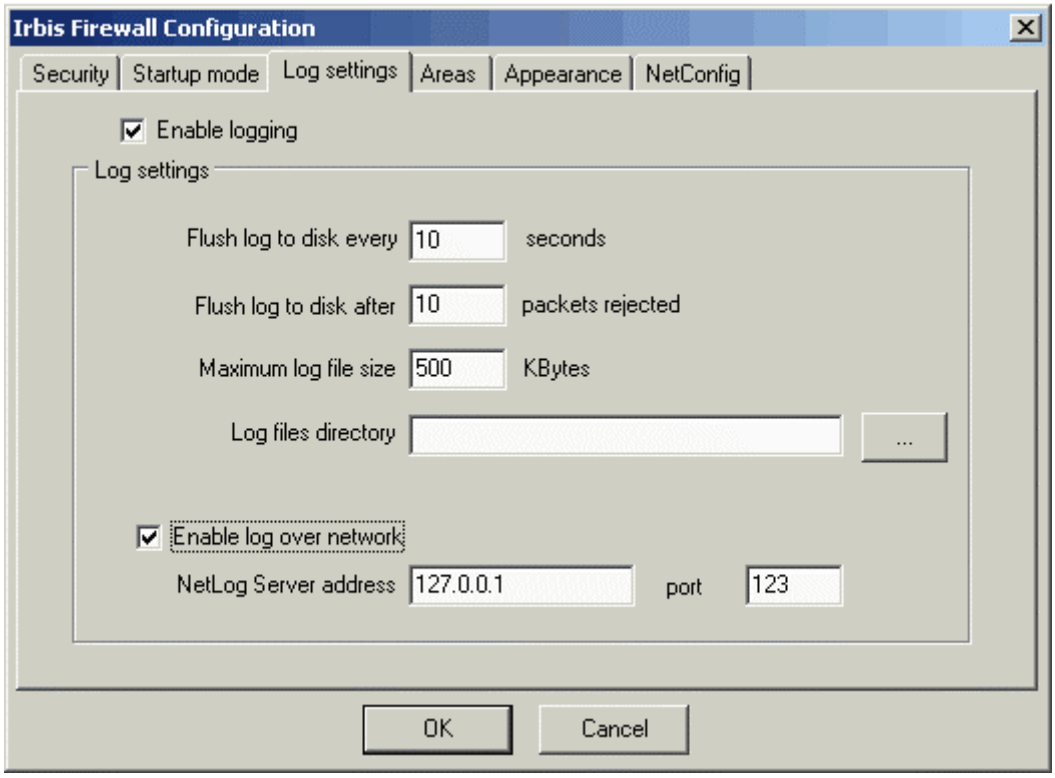
The **Startup mode** panel allows you to manage the **Irbis firewall** startup and execution mode. This panel is divided into two parts. The top part allows you to select the execution mode: **Service application** mode (works only on Microsoft Windows 2000/XP) or **Standalone application** mode (the only mode available in Microsoft Windows ME). The lower part allows you to run Irbis Firewall startup immediately after system boots up.

Service is a special Windows 2000/XP application that can be run without user interaction, even when user is not logged in. Standalone application interacts with user so it can be run only if user is logged into the system.



Log Settings

The **Log settings** panel allows you to manage the log settings of Irbis Firewall. Irbis Firewall log system can collect all the packets rejected by the filtration rules. The **Log settings** panel allows you to manage the log saving frequency and log file sizes.



Enable logging
Enables/disables packet logging.

Flush buffer after ... packets rejected
Sets the maximum number of packets that can be stored in the buffer without flushing them to hard drive.

Flush buffer every ... seconds
Sets the maximum time limit between two buffer flushes.

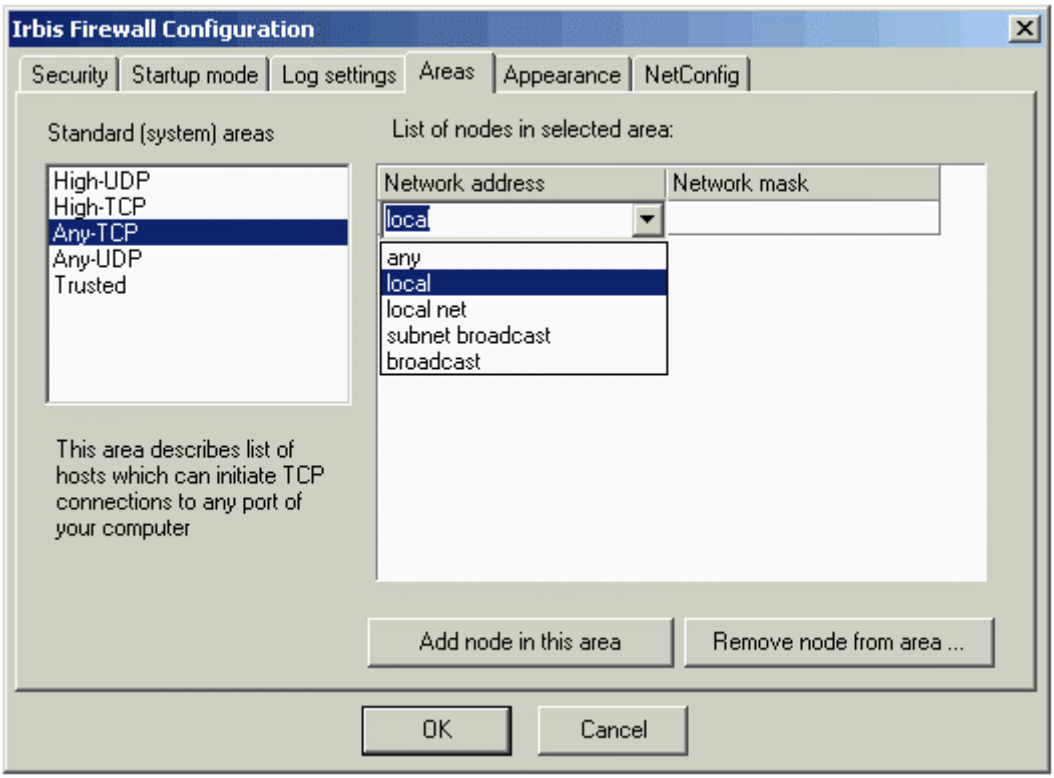
Maximum log file size
Sets the maximum log file size. When this size is reached, current log file renamed into the form of **YYYYMMDDHHmmSS.DMP**. Afterwards these files can be reached using the Irbis Firewall log viewer utility.

Log files directory
Sets the directory to store Irbis Firewall log files.

Enable log over network
Enables NetLog feature. Using this feature, Irbis Firewall can store log files on the remote log server. This option is available for **Irbis Firewall Enterprise Suite** and for **Irbis Firewall Enterprise Client**.

Areas

The **Areas** panel allows you to manage areas without use of advanced configuration options.



Standard Areas
Contains list of all the defined areas.

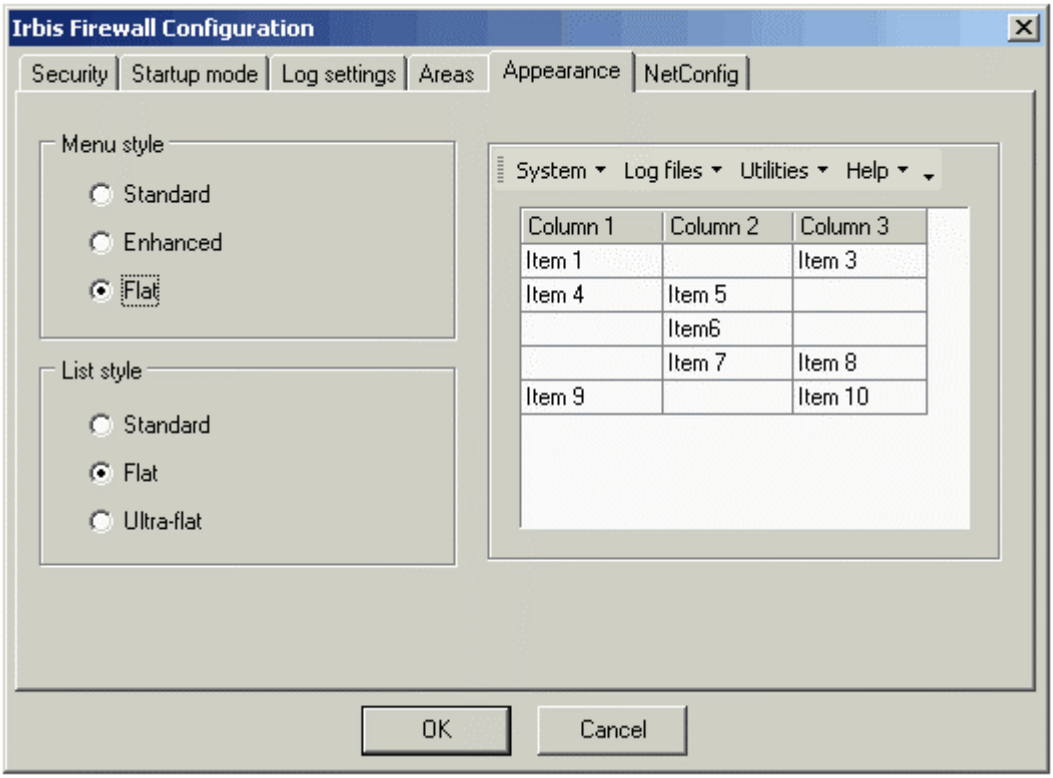
List of nodes in selected area
Contains list of all nodes that are included in the selected area.

Add node in this area
Adds a new node to the selected area. Node can be an IP-address of a computer or a subnet, or a special address

Remove node from area
Removes the selected node from the area.

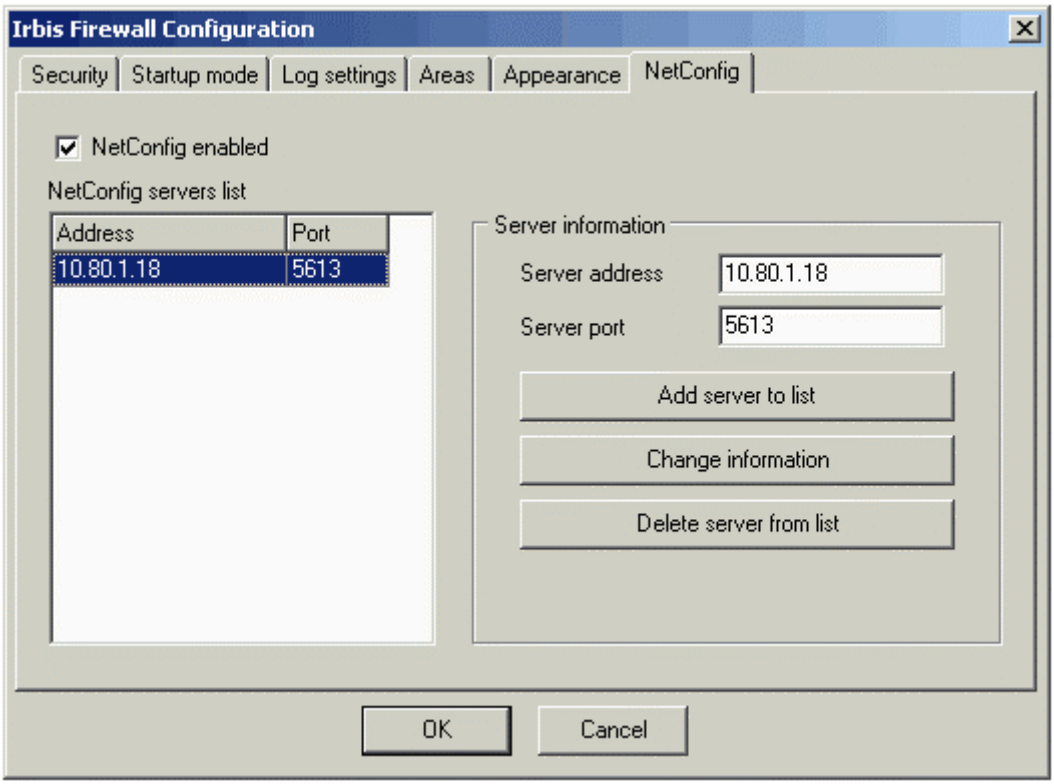
Appearance

The **Appearance** panel allows you to set your visual preferences for user interface controls.



NetConfig

The **NetConfig** panel allows you to set the Irbis Firewall automatic network configuration options. Using this panel you may enable or disable NetConfig feature and/or fill the list of NetConfig servers.



NetConfig enabled
Activates/deactivates the network configuration mode.

Add server to list
Adds a new server address to the list of servers where configuration can be obtained from.

Change information
Replaces a server selected in the list with a new one.

Delete server from list
Removes the selected server from the list

NetConfig server list
This list contains addresses and port numbers of the servers where Irbis Firewall configuration can be obtained from.

This panel is available only for **Irbis Firewall Enterprise Suite**.

HTTP Proxy Server Configuration Dialog

The **Proxy Server Configuration Dialog** allows you to define parameters, access control lists, and access control expressions used by the proxy server

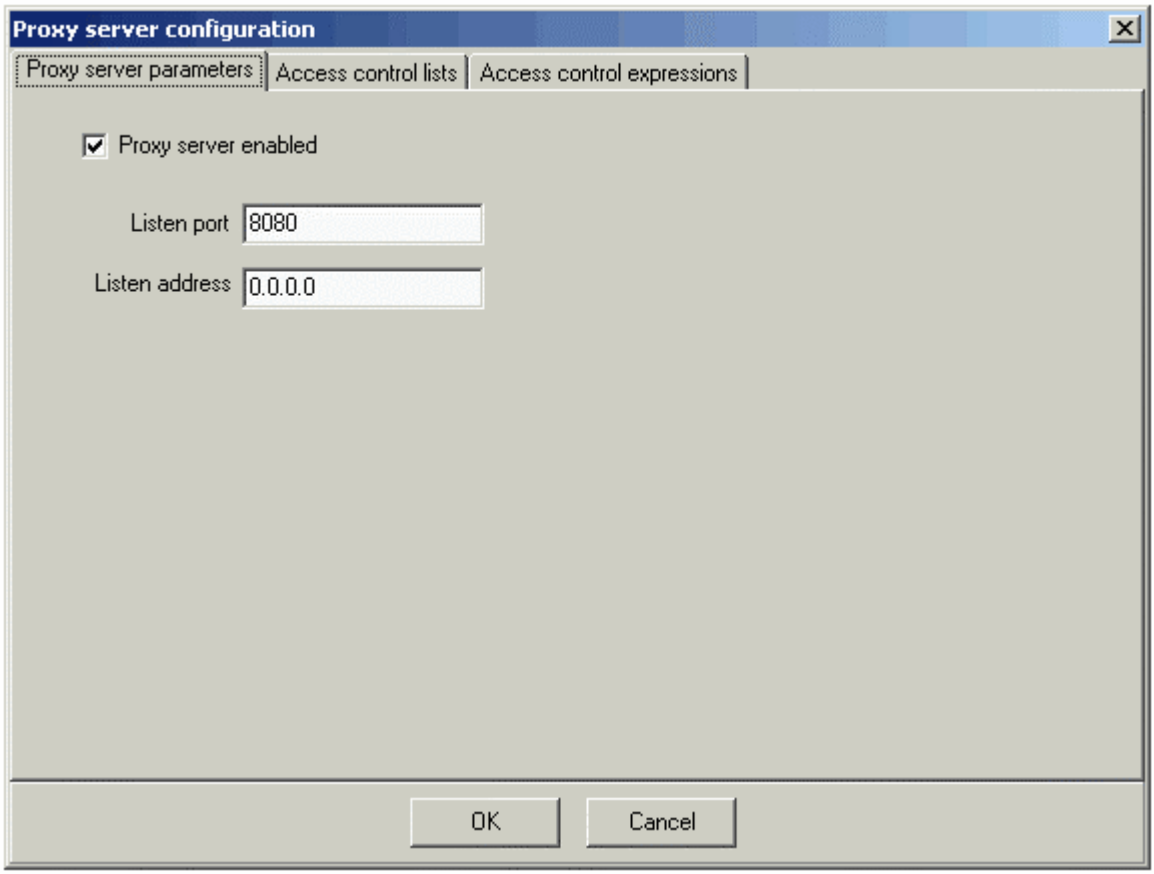
Proxy Server Parameters
This panel allows you to set the binding address and the port number used by the proxy server, and enable or disable the proxy server itself.

Access Control Lists
This panel allows you to manage the access control lists.

Access Control Expressions
This panel allows you to manage the access control expressions.

Proxy Server Parameters

The **Proxy Server Parameters** panel allows you to set the binding address and the port number used by the proxy server, and enable or disable the proxy server itself.



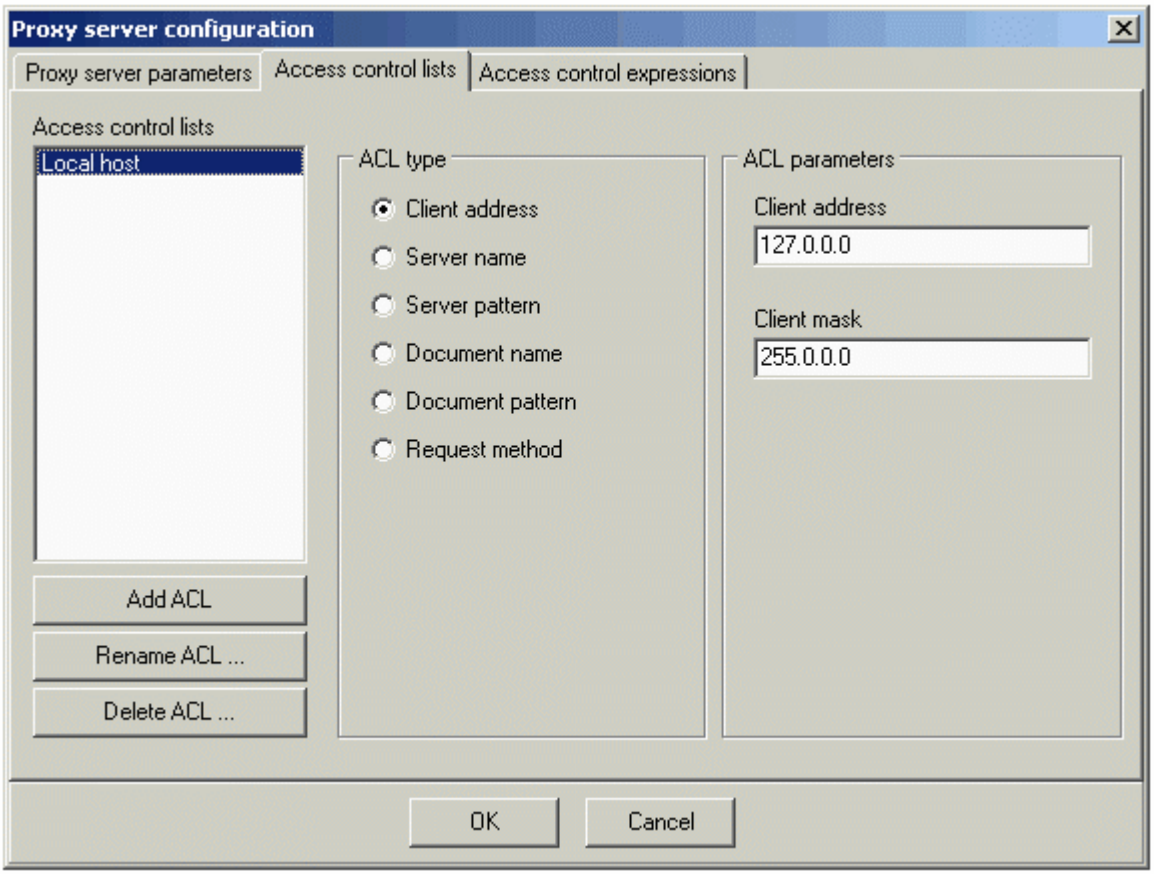
Proxy server enabled
Enables/disables the embedded proxy server.

Listen port
Defines the listen port number used by the proxy server. This number should be also declared in your browser settings as your proxy server port.

Listen address
Defines the listen address used by the proxy server. This address should be also declared in your browser settings as your proxy server address.

Access Control Lists

The **Access Control Lists** panel allows you to define the access control lists used by the Irbis Firewall embedded proxy server while analyzing requests.



Access control lists
Enumerates the existing access control lists.

Add ACL
Creates a new access control list.

Rename ACL
Allows you to rename the selected access control list.

Delete ACL
Removes the selected access control list.

ACL type
Changes the type of the selected ACL.

ACL parameters
The controls of this group depend on the selected type and allows you to set the selected ACL parameters.

The following ACL types are available:

Client address
Client IP address based ACL. This ACL type has two parameters: **IP address** and the **subnet mask** of the client computer. A request is accepted by this ACL type only if it was sent from the computer that is in the declared subnet.

Server name

Server name based ACL. This ACL type requires the **name of the server**, from which a document is requested. A request is accepted by this ACL type only if a document is requested from the declared server.

Server pattern
Server name substring based ACL. The only parameter for this ACL type is the **substring**, by which the **server name** is searched. A request is accepted by this ACL type only if server name contains the declared substring.

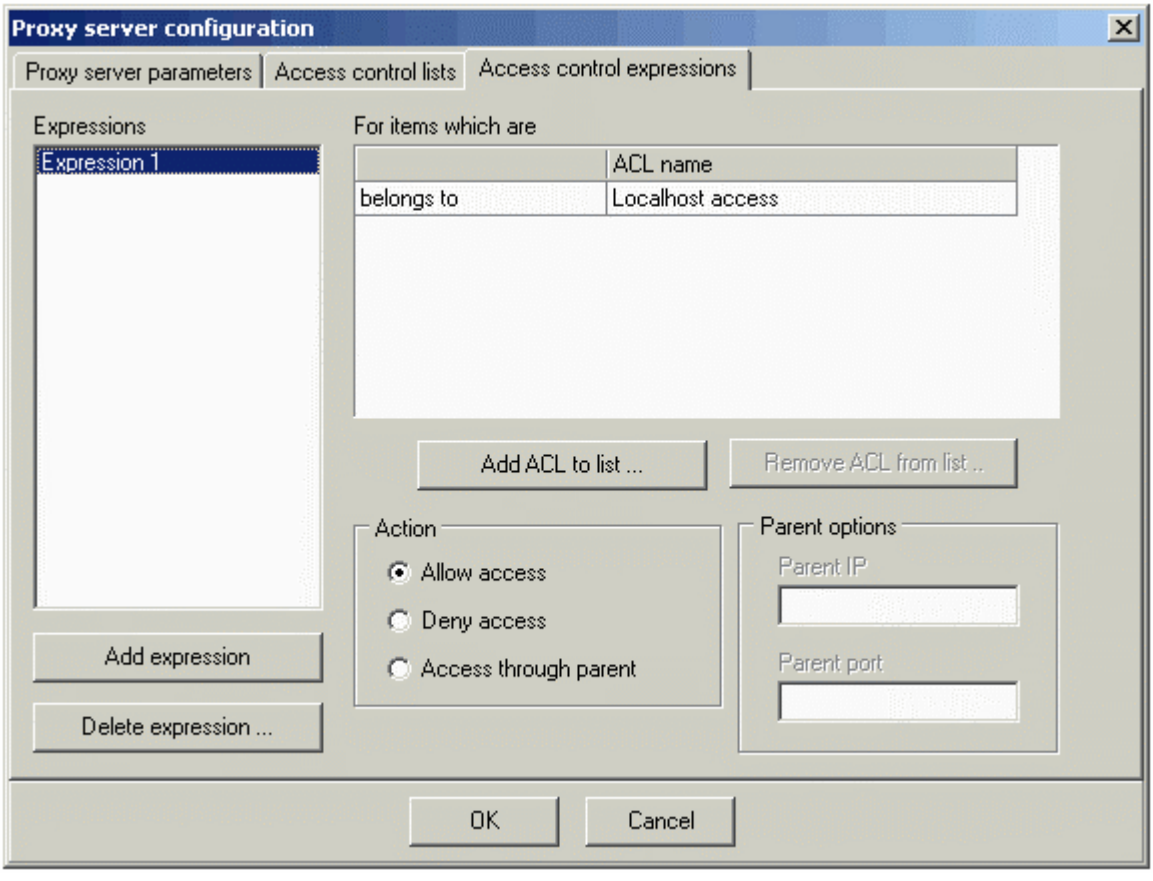
Document name
Document name based ACL. This ACL type takes the **requested document name** as a parameter. A request is accepted by this ACL type only if the requested document name matches the declared name.

Document pattern
Document name substring based ACL. The parameter for this ACL type is the **substring**, by which the **requested document** is searched. A request is accepted by this ACL only if the requested document name contains the declared substring.

Request method
Request method based ACL. The parameter for this ACL type is the **request method** (GET/POST/HEAD). A request is accepted by this ACL only if the request method matches the declared method.

Access Control Expressions

The **Access Control Expressions** panel allows you to manage expressions used by the Irbis Firewall for analyzing document requests received from the client computer.



Expressions
Lists all the existing expressions.

Add expression
Creates a new expression.

Delete expressions
Removes the selected expression.

For items which are
Lists the access control lists, by which the request should be accepted/not accepted. Setting the first column value to **not belongs to** sets the inverse flag for the ACL, i.e. the request should not be accepted by this ACL in order the selected action (see below) to be performed.

Add ACL to list
Adds an access control list to the selected expression.

Delete ACL from list
Removes the selected access control list from the expression.

Action
This switch defines the action executed if a request is accepted/not accepted by proper ACLs.

Allow access
Forces Irbis Firewall embedded proxy server to execute the request and return the requested data to the client.

Deny access
Forces Irbis Firewall embedded proxy server not to execute the request and return a notification to the client.

Access through parent
Forces Irbis Firewall embedded proxy server to pass the request to the parent proxy server.

Parent options
This group becomes available only if **Action** is set to **Access through parent**. It allows you to define the address and the port number of the parent proxy server.

NetConfig Technology

NetConfig is the Irbis Firewall feature designed for working in local networks. Using **NetConfig** you can manage configurations of multiple Irbis Firewall instances from one computer. With **NetLog** you can also collect Irbis Firewall logs from multiple computers on one **NetLog** server.

In order to use NetConfig and NetLog features you are to meet some requirements. The first is that at least one computer should run **Irbis NetConfig** server. This software manages Irbis configurations obtained from other computers. The second requirement is that client computers should run **Irbis Firewall Enterprise Suite** or **Irbis Firewall Enterprise Client**, because **Irbis Firewall Standard Suite** doesn't support **NetConfig** and **NetLog** features.

When starting Irbis Firewall having the **NetConfig** feature activated, Irbis Firewall tries to connect to the **NetConfig** server and obtain the configuration. If configuration was obtained successfully Irbis Firewall uses it for the current session, otherwise (if configuration was not loaded) Irbis Firewall uses local configuration.

Irbis NetConfig Server Manager

Irbis NetConfig Server is included into the **Irbis Firewall Enterprise Suite**.

This program consists of two modules: **Irbis NetConfig Server Manager** and **Irbis NetConfig Service**. The first module allows you to manage configurations for remote NetConfig clients and the second one is used internally when **Irbis NetConfig Server** is working in the service mode.

To call the **Irbis NetConfig Server Manager** click the **Start** button, then go to the **Programs | Irbis Firewall Enterprise Suite** menu and select **Irbis NetConfig Manager**.

Manager window is divided into the following panels:

Configuration over Network
Use this panel to manage main NetConfig server parameters.

Logs over Network
This panel allows you to define the NetLog server parameters.

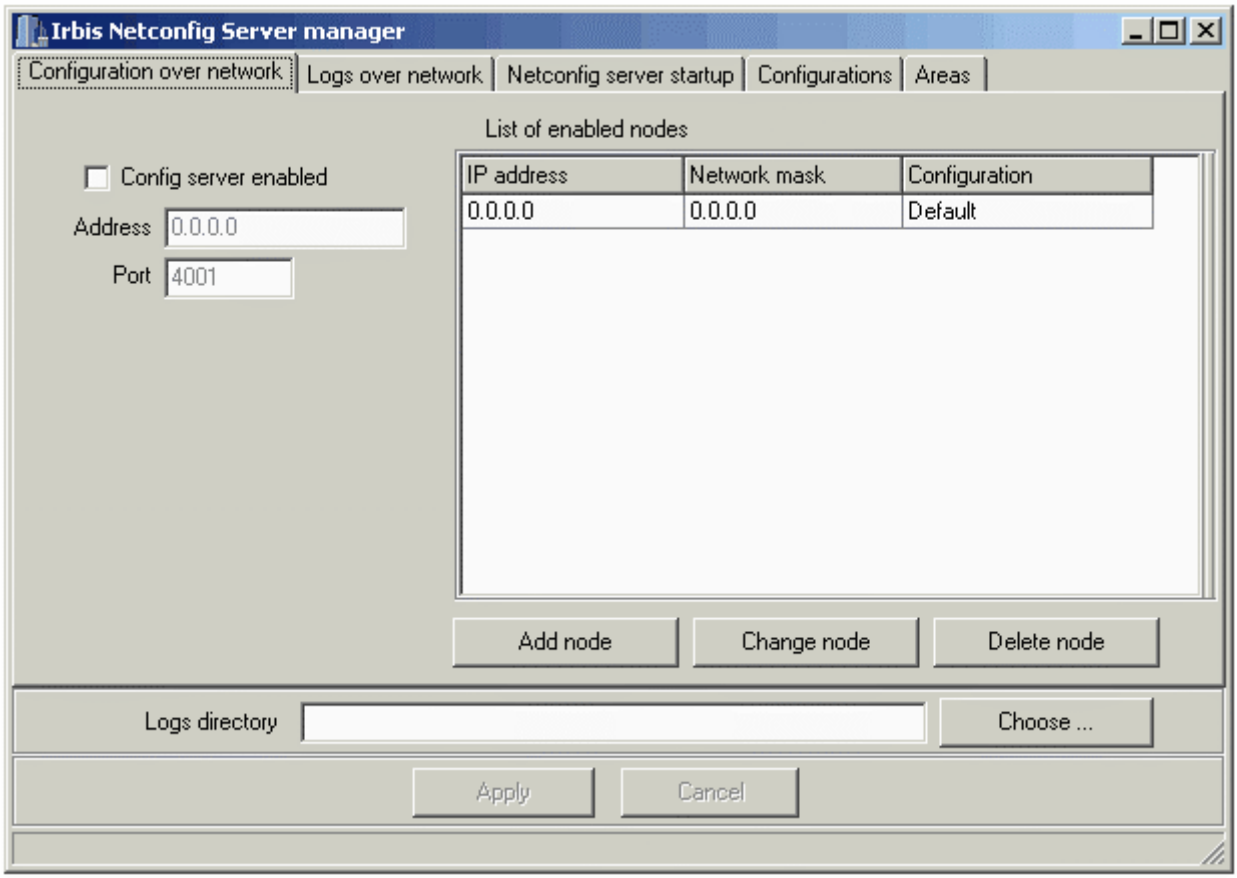
NetConfig Server Startup
This panel defines the NetConfig execution mode.

Configurations
Use this panel for managing configurations for the NetConfig clients.

Areas
This panel allows you manage areas.

Configuration over Network

The **Configuration over Network** panel allows you managing NetConfig server behavior and access control. Using this panel you can set the NetConfig server listening address and port number, and declare the list of the clients to access to the server.



Config server enabled
Enables/disables NetConfig server.

Address
Sets listening address for the NetConfig server.

Port
Sets listening port number for the NetConfig server.

List of enabled nodes
Lists all the client computers granted to use this server as a NetConfig server and the configurations obtained by these computers.

IP address
The IP address of the client computer or subnet.

Network mask
The subnet mask of the client computer.

Configuration
The name of the configuration obtained by the client computer.

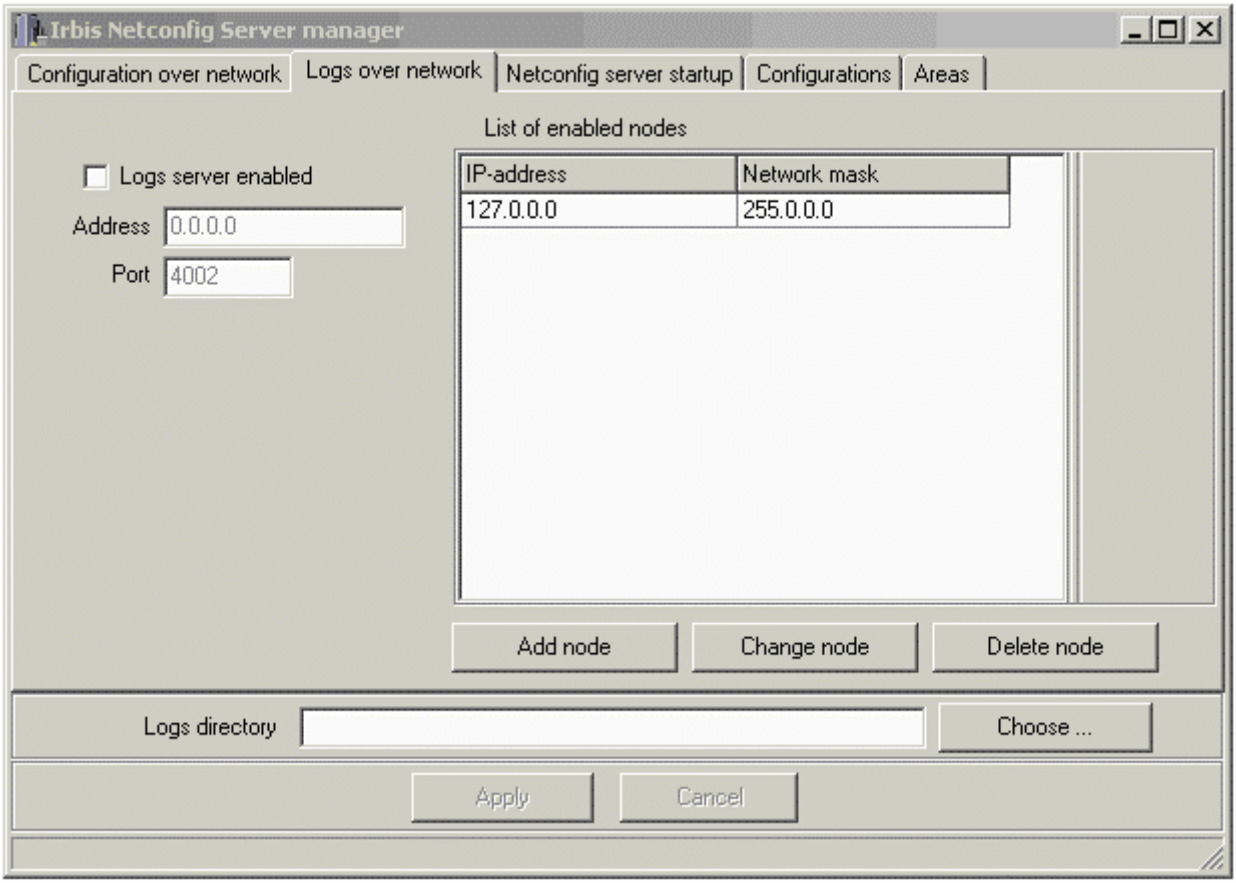
Add node
Adds a new NetConfig client.

Change node
Allows you to change the IP address, network mask, or the configuration for the selected client.

Delete node
Removes the selected client from the list.

Logs over Network

The **Logs over Network** panel allows you to manage the parameters of the NetLog server. These parameters include the server listening address, server listening port number and the list of the clients, which are able to save Irbis Firewall logs using the server.



Logs server enabled
Enables/disables NetLog server.

Address
Sets listening address for the NetLog server.

Port
Sets listening port number for the NetLog server.

List of enabled nodes
Lists all the client computers granted to use this server as a NetLog server and which logs can be obtained by the server.

IP address
The IP address of the client computer or subnet.

Network mask
The subnet mask of the client computer.

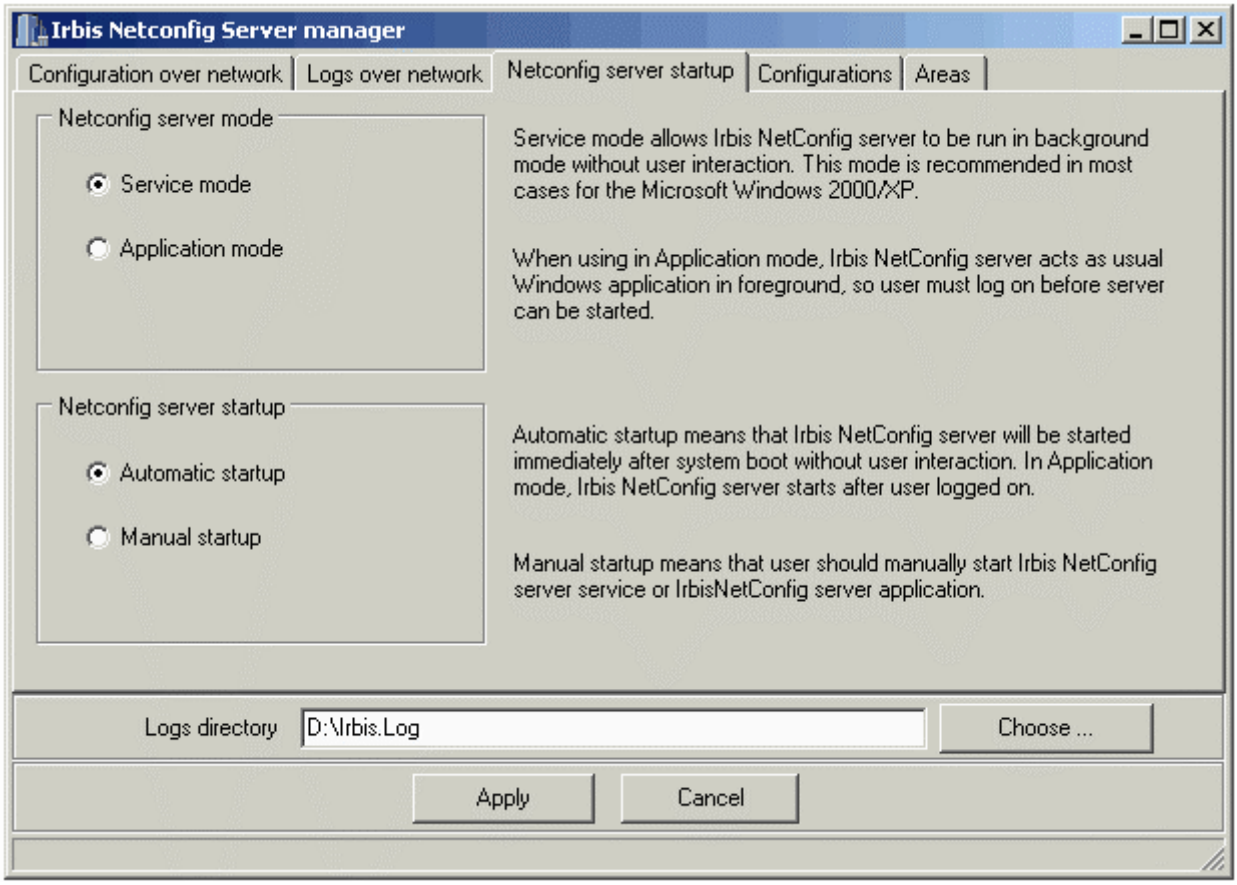
Add node
Adds a new NetLog client.

Change node
Allows you to change the IP address or the network mask for the selected client.

Delete node
Removes the selected client from the list.

NetConfig Server Startup

The **NetConfig Server Startup** panel allows you to set the startup modes of the NetConfig and NetLog server. Two modes are available: the service mode and the application mode. In the service mode the server can start up automatically without logging to Windows (if **Automatic startup** is on), and in the application mode the server is available only when **Irbis NetConfig Server Manager** is running.



Service mode
Switches the NetConfig and NetLog server into the service mode.

Application mode
Switches the NetConfig and NetLog server into the application mode.

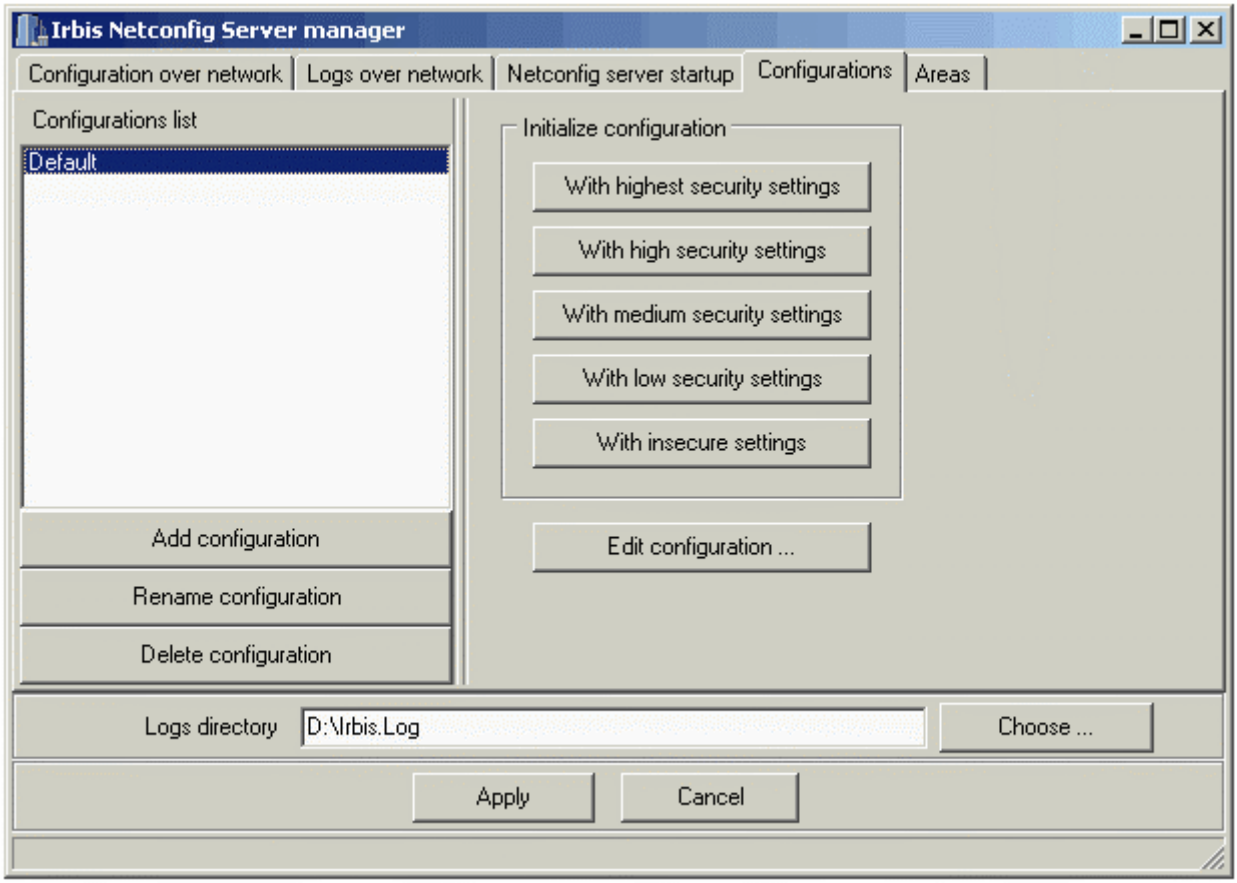
Automatic startup
Forces server to start automatically without logging to Windows in service mode or right after logging.

Manual startup

Forces server to be started manually as a service or along with the NetConfig Server Manager.

Configurations

The **Configurations** panel allows you to manage configurations. Any configuration may be obtained by any number of clients;
the client may obtain only one configuration. Each configuration should have its own unique name. All configurations share the same area set.



Configurations
Lists all the defined configurations.

Add configuration
Creates a new empty configuration.

Rename configuration
Allows you to rename the selected configuration.

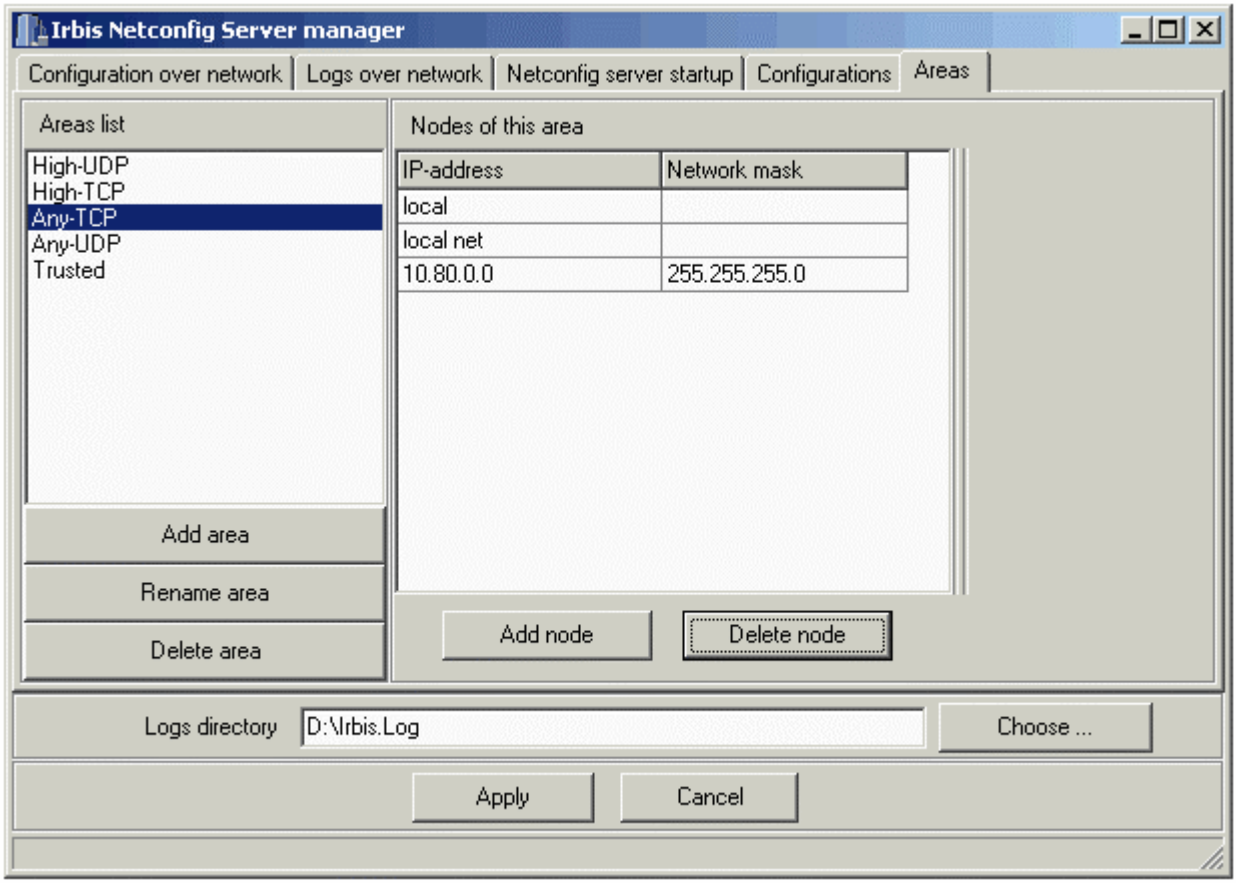
Delete configuration
Removes the selected configuration.

Edit configuration
Opens the dialog window for editing the selected configuration. This dialog window is similar to the Custom Security Level Configuration Dialog.

Initialize configuration
These buttons set the selected configuration to one of the pre-defined security levels. See the Security panel of the Irbis Firewall Configuration Dialog for details.

Areas

The **Areas** panel allows you to manage the NetConfig server areas. All configurations share the same area set, so you can easily modify all configurations from one point.



Create area
Creates a new area.

Rename area
Allows you to rename the selected area.

Delete area
Removes the selected area.

Add node
Adds a new address into the selected area

Delete node
Removes the selected address from the area.

Configuring NetConfig Client

If you want to use Irbis Firewall **NetConfig** and **NetLog** features, client computers should run **Irbis Firewall Enterprise Suite** or **Irbis Firewall Enterprise Client**. To activate these features use the NetConfig and the Log Settings panels of the Irbis Firewall Configuration Dialog.

To activate NetConfig

1. Open the NetConfig panel of the Configuration Dialog.
2. Set the **NetConfig enabled** option on.
3. Set the listening address of the NetConfig server in the **Server address** box.
4. Set the listening port number of the NetConfig server in the **Server port** box.
5. Click the **Add server to list** button to add a server with the parameters you set to the list of the NetConfig servers.

Listening address and port number are defined by the system administrator in the Irbis NetConfig server configuration.

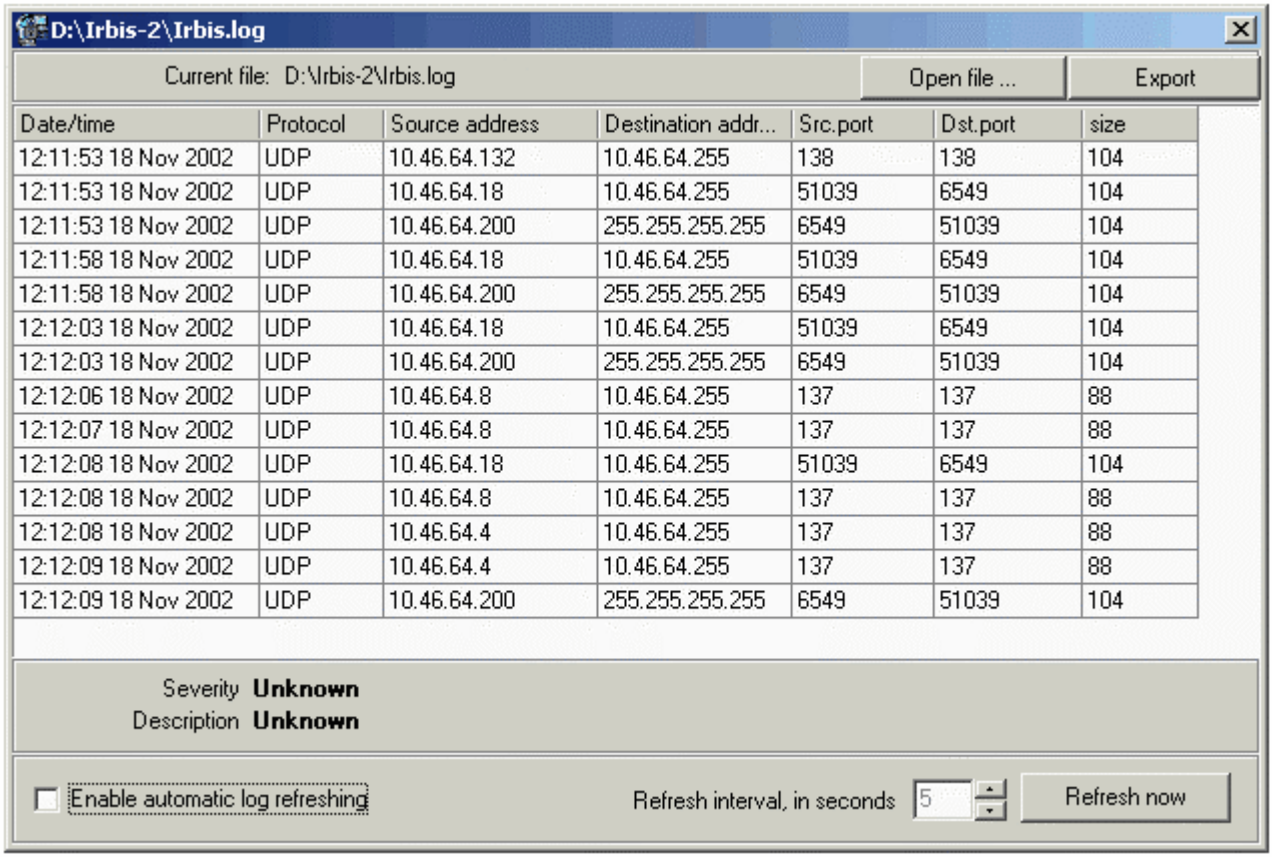
To activate NetLog

1. Open the Log Settings panel of the Configuration Dialog.
2. Set the **Enable log over network** option on.
3. Set the listening address of the NetConfig server in the **NetLog server address** box.
4. Set the listening port number of the NetConfig server in the **port** box.

Irbis Firewall Logs

Irbis Log View

Irbis Firewall Log window allows you to view the list of IP packets rejected by Irbis Firewall. Packets are logged only if the **Enable logging** switch is on in the Log Settings panel of the Irbis Firewall Configuration Dialog.



Open file
Use this button to load a previously saved log file.

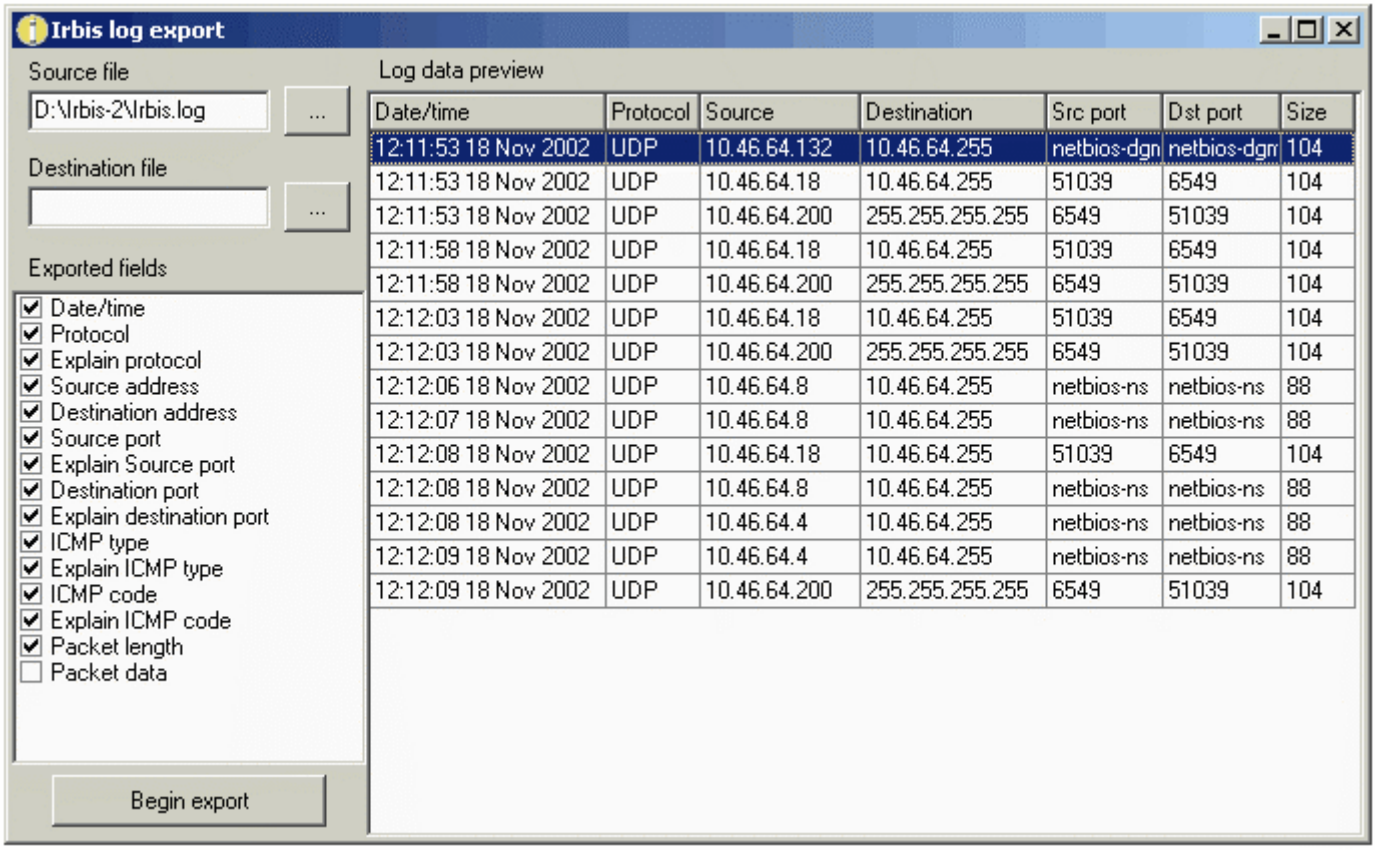
Export
Exports the current log from the internal Irbis Firewall format to the text file. See **Irbis Log Export** for details.

Enable automatic log refreshing
Enables automatic reload of the log file with an interval defined by the **Refresh interval, in seconds** option. The minimal interval is 5 seconds, and the maximum is 300 seconds.

Refresh now
Reloads the current log file.

Irbis Log Export

The **Irbis Log Export** utility exports the Irbis Firewall log files from the internal format to the text files. Using this utility, you can view the content of the log files and export them into readable format.



Source file
Displays the name of the loaded log file. Click the [...] button for browsing.

Destination file
Sets the result *.txt file name. Click the [...] button for browsing.

Begin export
Starts the export procedure. When export complete a notifying message box is shown.

Export fields
Lists all the log fields available for export. A flag next to each field indicates whether a field is exported or not. All fields are selected default; to exclude a field from the exported fields remove a flag next to the field name.