



# **IKARUS security.proxy**

Manual



## Contents

<b>1</b>	<b>General Information on IKARUS security.proxy</b>	<b>11</b>
1.1	Introduction . . . . .	11
1.2	Product Details . . . . .	11
1.3	<b>IKARUS security.proxy</b> Feature List . . . . .	11
<b>2</b>	<b>Installation</b>	<b>13</b>
2.1	Requirements . . . . .	13
2.2	Installation on Microsoft Windows Systems . . . . .	13
2.3	Installing on a Linux System . . . . .	13
2.4	Licensing . . . . .	14
2.5	Stopping and Starting the service . . . . .	14
2.5.1	On Microsoft Windows Systems . . . . .	14
2.5.2	On Linux . . . . .	14
2.6	Using the <b>IKARUS security.proxy</b> . . . . .	14
<b>3</b>	<b>Configuration</b>	<b>15</b>
3.1	Edit Menu . . . . .	15
3.2	Help Menu . . . . .	16
3.3	Server Information . . . . .	18
3.4	Global Settings . . . . .	19
3.5	Alerting . . . . .	21
3.6	Auto-Update . . . . .	23
3.7	Logging . . . . .	24
3.8	User Administration . . . . .	25
3.8.1	Global Users . . . . .	25
3.8.2	Remote Manager . . . . .	25

3.9	Web Settings . . . . .	26
3.9.1	HTTP Proxy . . . . .	27
3.9.2	FTP Proxy . . . . .	28
3.9.3	Next Proxy . . . . .	29
3.9.4	Scan Settings . . . . .	31
3.9.5	Access List . . . . .	37
3.10	Mail Settings . . . . .	40
3.10.1	Scan Rules . . . . .	41
3.10.2	SMTP . . . . .	48
3.10.3	TSMTP - the transparent SMTP Proxy . . . . .	53
3.10.4	POP3 proxy . . . . .	54
3.10.5	IMAP4 Proxy . . . . .	55
3.10.6	NNTP Proxy . . . . .	57
3.11	Your Network . . . . .	58
3.12	Clustering . . . . .	58
3.13	WCCP . . . . .	60
3.14	Reporting . . . . .	61
3.14.1	Global Settings . . . . .	61
3.14.2	Auto-Reporting . . . . .	63
3.14.3	Creating a New Report . . . . .	64
3.14.4	Defined Reports . . . . .	65
3.15	Log Files . . . . .	69
3.16	Config File . . . . .	69
3.17	Virus List . . . . .	70
3.18	Activity Monitor . . . . .	71
3.19	Show Reports . . . . .	72

<b>4</b>	<b>Using the IKARUS security.proxy</b>	<b>74</b>
4.1	Using <b>IKARUS security.proxy</b> as an MX Gateway . . . . .	74
4.1.1	Overview . . . . .	74
4.1.2	Prerequisites . . . . .	74
4.1.3	Settings in <b>IKARUS security.proxy</b> . . . . .	74
4.2	Using <b>IKARUS security.proxy</b> as a Mail Relay . . . . .	75
4.2.1	Overview . . . . .	75
4.2.2	Prerequisites . . . . .	75
4.2.3	Settings in <b>IKARUS security.proxy</b> . . . . .	76
4.3	The URL Filter . . . . .	76
4.3.1	How to Configure the URL Filter? . . . . .	77
4.3.2	Branding . . . . .	79
4.4	Sending E-Mail over TLS . . . . .	80
4.4.1	Overview . . . . .	80
4.4.2	Prerequisites . . . . .	80
4.4.3	How to Verify if TLS is enabled . . . . .	81
4.5	How to Configure for LDAP Authentication . . . . .	81
4.5.1	Overview . . . . .	81
4.5.2	Prerequisites . . . . .	81
4.5.3	LDAP Path Settings . . . . .	82
4.5.4	Creating Permission Sets for LDAP Groups . . . . .	83
4.5.5	Creating Access Lists for LDAP Authentication . . . . .	83
4.5.6	Using LDAP Authentication in Your Browser . . . . .	84
4.6	Safe Web Browsing with <b>IKARUS security.proxy</b> . . . . .	84
4.6.1	How to Browse the Web using <b>IKARUS security.proxy</b> . . . . .	84
4.6.2	How to Set up a Permission Set . . . . .	87

4.6.3	How to Allow or Deny Specific Pages, Domains, or URLs . . . . .	89
4.6.4	How to Allow or Deny Specific Files . . . . .	89
4.6.5	How to Allow or Deny Specific Contents . . . . .	90
4.6.6	What is the Purpose of Browser Lists? . . . . .	90
4.6.7	How to Use the Permission Set Properly . . . . .	91
4.6.8	How to Use the Custom Permission Sets . . . . .	91
4.7	Greylisting . . . . .	92
4.8	Reporting . . . . .	93
4.8.1	How to Create a Report . . . . .	93
4.8.2	How to Edit a Report . . . . .	94
4.8.3	How to View a Report . . . . .	95
4.8.4	How to Send a Report automatically . . . . .	96
<b>5</b>	<b>IKARUS security.proxy FAQ</b>	<b>98</b>
<b>6</b>	<b>Glossary</b>	<b>100</b>

## List of Figures

1	Edit menu . . . . .	15
2	Help menu . . . . .	17
3	Server Information . . . . .	19
4	Global settings . . . . .	20
5	Alerting . . . . .	22
6	Auto-Update . . . . .	23
7	Logging . . . . .	24
8	Global users . . . . .	25
9	Remote manager . . . . .	26
10	HTTP proxy . . . . .	27
11	FTP proxy . . . . .	29
12	Next proxy . . . . .	30
13	Lists . . . . .	31
14	Sample list . . . . .	32
15	Sample content type list . . . . .	33
16	Permissions . . . . .	34
17	Permission Sets . . . . .	35
18	Conditions for permission sets . . . . .	37
19	Access list . . . . .	38
20	NTLM/Kerberos . . . . .	38
21	Priority list . . . . .	40
22	Scan rules overview . . . . .	41
23	Sample scan rule . . . . .	42
24	Virus filter . . . . .	43

25	Attachment filter . . . . .	44
26	SPAM filter . . . . .	45
27	SPAM rules . . . . .	47
28	SMTP . . . . .	49
29	Greylisting . . . . .	51
30	Routes . . . . .	52
31	TSMTP . . . . .	53
32	POP3 . . . . .	54
33	IMAP4 . . . . .	56
34	NNTP . . . . .	57
35	Your Network settings . . . . .	58
36	Clustering . . . . .	59
37	WCCP . . . . .	60
38	Reporting: Global Settings . . . . .	61
39	Reporting: Auto-Reporting . . . . .	63
40	Reporting: Create a new report . . . . .	64
41	Reporting: Defined reports . . . . .	65
42	Reporting: Chart types and layout types . . . . .	66
43	Reporting: Filter settings (Web) . . . . .	66
44	Reporting: Filter settings (Mail) . . . . .	68
45	Log files . . . . .	69
46	Configuration file . . . . .	70
47	Virus List . . . . .	70
48	ActivityMonitor . . . . .	71
49	Show Report . . . . .	72
50	Overview MX Gateway . . . . .	74



51	Overview Mail Relay . . . . .	75
52	URL filter . . . . .	77
53	URL filter categories . . . . .	78
54	Permissions . . . . .	78
55	Permission sets . . . . .	79
56	Definition of LDAP path . . . . .	82
57	Creating permission sets for LDAP groups . . . . .	83
58	LDAP access list . . . . .	84
59	HTTP proxy settings . . . . .	85
60	Creating permission sets . . . . .	86
61	Setting Access list . . . . .	86
62	Configure permission set . . . . .	87
63	Configure URL list . . . . .	88
64	Use URL list in permission set . . . . .	88
65	Use URLs/files in permission sets . . . . .	89
66	Configure Browser list . . . . .	90
67	Custom Permission Sets . . . . .	91
68	Configure permission set . . . . .	92
69	Reporting menu . . . . .	93
70	Reporting: New report . . . . .	94
71	Reporting: Edit . . . . .	95
72	Reporting: Show . . . . .	96
73	Reporting: Auto-Reporting . . . . .	97

## List of Tables

1	Edit menu . . . . .	16
2	Help menu . . . . .	18
3	Server Information . . . . .	19
4	Global settings . . . . .	20
5	LDAP . . . . .	21
6	Alerting . . . . .	22
7	Auto-Update . . . . .	23
8	Logging . . . . .	24
9	Remote manager . . . . .	26
10	HTTP proxy . . . . .	28
11	FTP proxy . . . . .	29
12	Next proxy - proxy chain . . . . .	30
13	Lists . . . . .	31
14	Content type information . . . . .	34
15	Permissions . . . . .	36
16	Access list . . . . .	39
17	Virus filter . . . . .	43
18	Attachment filter . . . . .	44
19	SPAM filter . . . . .	46
20	SPAM rules . . . . .	47
21	"field" values for SPAM rules . . . . .	48
22	SPAM classification results . . . . .	48
23	SMTP . . . . .	50
24	Greylisting . . . . .	51

25	Routes . . . . .	52
26	TSMTTP settings . . . . .	54
27	POP3 settings . . . . .	55
28	IMAP settings . . . . .	56
29	NNTP settings . . . . .	57
30	Your Network settings . . . . .	58
31	Clustering . . . . .	59
32	WCCP . . . . .	60
33	Reporting: Global Settings . . . . .	62
34	Reporting: Auto-Reporting . . . . .	63
35	Reporting: Create new report . . . . .	64
36	Reporting: Defined reports . . . . .	65
37	Reporting: Filter settings (Web) . . . . .	67
38	Reporting: Filter settings (Mail) . . . . .	68
39	Show Reports . . . . .	73
40	Glossary . . . . .	100

# 1 General Information on IKARUS security.proxy

## 1.1 Introduction

Today, any business not providing data exchange over the Internet is practically without a chance in its market. Whether you are an SMB, a global player, an educational or public institution, or even an ISP, you will almost certainly depend on a functioning Internet connection in your day-to-day work. The prevalence of the World Wide Web leads us to take it for granted; on the other hand, we tend to forget that its predominant tools – e-mail and the Internet – are the preferred gateways of malware attacks.

During the next years, those attacks will become more frequent and increasingly sophisticated. Worse still, businesses inadvertently contribute to the spread of hazardous malware by letting their employees freely visit infected web sites, download files from remote locations, or even send files from the company network to the Internet.

The effects on the network infrastructures are often substantial: spam keeps slowing down the servers. This puts valuable data at significant risk, wastes employees' precious work time, and also generates avoidable costs.

## 1.2 Product Details

**IKARUS security.proxy** is a software-based content-security solution. It integrates into your internal network with minimum effort and can be implemented on the gateway level. The solution is designed for protecting small businesses with a limited number of users as well as large enterprises with several thousand clients.

Thanks to its unlimited compatibility, **IKARUS security.proxy** can be used in combination with any firewall. Installation packages are available for Microsoft Windows and Linux (RPM package). The **IKARUS security.proxy** versions for Microsoft Internet Security & Acceleration (ISA) Server and Microsoft Threat Management Gateway (TMG) are highly innovative: They allow for transparently integrating the comprehensive feature set of our content-security solution with MS ISA/TMG Server.

All versions of **IKARUS security.proxy** are also available as turnkey solutions on SecureGUARD appliances.

## 1.3 IKARUS security.proxy Feature List

For a complete and updated list of **IKARUS security.proxy** features, visit the **IKARUS** website.

Key features include:

- Built-in **IKARUS** AntiVirus ScanEngine
- Virus protection for web protocols (HTTP, FTP over HTTP, FTP) and mail protocols (SMTP, IMAP, POP3, NNTP)
- AntiSPAM: **IKARUS** AntiSPAM Engine protecting mail protocols (SMTP, IMAP, POP3, NNTP)
- Greylisting support, SPF support (SMTP)
- TLS support (SMTP)

- Simple creation of access profiles using URL, file, and content-type lists
- Access control using IP-address groups
- IPv6 support for outgoing connections
- Supported authentication types: Basic Proxy Authentication, LDAP Authentication and NTLM/Kerberos Authentication (last one is Windows-only)
- Fully automated incremental update (every 10 minutes) for antivirus, anti-spam, and URL filter databases as well as the **IKARUS** ScanEngine and the **IKARUS** AntiSPAM Engine
- Custom creation of administrative access levels
- Activity Monitor (**IKARUS security.proxy Configuration Center**)
- Comprehensive logging of all activities
- Reporting functionality for a clear overview of the collected data; reports can also be generated and sent per e-mail automatically
- Setup packages for Microsoft Windows and Linux
- Version for Microsoft ISA/TMG
- Integration in existing management interface, ruleset applicable on existing ISA/TMG rules, transparent integration of AntiVirus und URL filter
- Available as pre-installed solution on SecureGUARD appliances

## 2 Installation

### 2.1 Requirements

Make sure that your system meets the following requirements before starting the **IKARUS security.proxy** installation:

- The user ID used for installing the system has administrative rights
- The system clock has the correct setting
- The network settings of the operating system (including the IP address, routing/default-gateway, and DNS settings) have been configured properly
- The system has sufficient free disk space
- The default ports of **IKARUS security.proxy** (TCP 8080, TCP 2100, TCP 15639) are available
- The firewall allows the transmission of the necessary protocols (HTTP, HTTPS, POP3, IMAP, NNTP, and SMTP) from inside the system
- The firewall allows for data reception on the required ports (management port: TCP 15639; web-proxy port: TCP 8080)
- The **IKARUS security.proxy** setup file appropriate for the OS (32-bit or 64-bit) is available
- An **IKARUS security.proxy** trial or full license is available

### 2.2 Installation on Microsoft Windows Systems

Installing **IKARUS security.proxy** on a Microsoft Windows system is straightforward. Double-clicking the setup file will install **IKARUS security.proxy** on your system. Simply follow the instructions provided by the wizard.

**Remark:** It is recommended to keep the default settings if possible.

During installation, you may enable your **IKARUS security.proxy** license. Alternatively, you can skip this step and enable the license at later time.

The installation of the **IKARUS security.proxy Configuration Center** works the same way.

### 2.3 Installing on a Linux System

For the installation of the **IKARUS security.proxy** on a Linux system there are RPM and DEB packages available. Each package comes as a 32-bit and 64-bit version.

```
> rpm -ivh IKARUSSecurityProxy-3.26.3rh5.x86_64.rpm
```

```
> dpkg -i IKARUSSecurityProxy-3.26.3_amd64.deb
```

## 2.4 Licensing

During the Windows installation process, you will be prompted to add a license. On Linux systems, you can do this on the command line after the installation process has finished.

The following sample shows the command line on a 64-bit Linux system:

```
# cd /opt/securityproxy/bin
# ./securityproxy_l64 -importlicense <licensefile>
```

## 2.5 Stopping and Starting the service

### 2.5.1 On Microsoft Windows Systems

When the installation is complete, the list of services installed on the system will include the service **securityproxy**. You can stop and restart it like any other service using the Administrative Tools.

### 2.5.2 On Linux

On a Linux system, the service **securityproxy** will be registered in the appropriate run levels. Stop and restart the service using a start script:

```
# /etc/init.d/securityproxy stop
# /etc/init.d/securityproxy start
```

or

```
# /etc/init.d/securityproxy restart
```

## 2.6 Using the IKARUS security.proxy

You can use **IKARUS security.proxy** immediately after installation. The only requirement is to configure a proxy on your Web client (Microsoft Internet Explorer, Mozilla Firefox, Opera, etc.). For that purpose, you need to enter the DNS name or IP address of your system and the appropriate TCP port 8080.

## 3 Configuration

### 3.1 Edit Menu

The Edit menu includes options for setting general **IKARUS security.proxy** parameters.

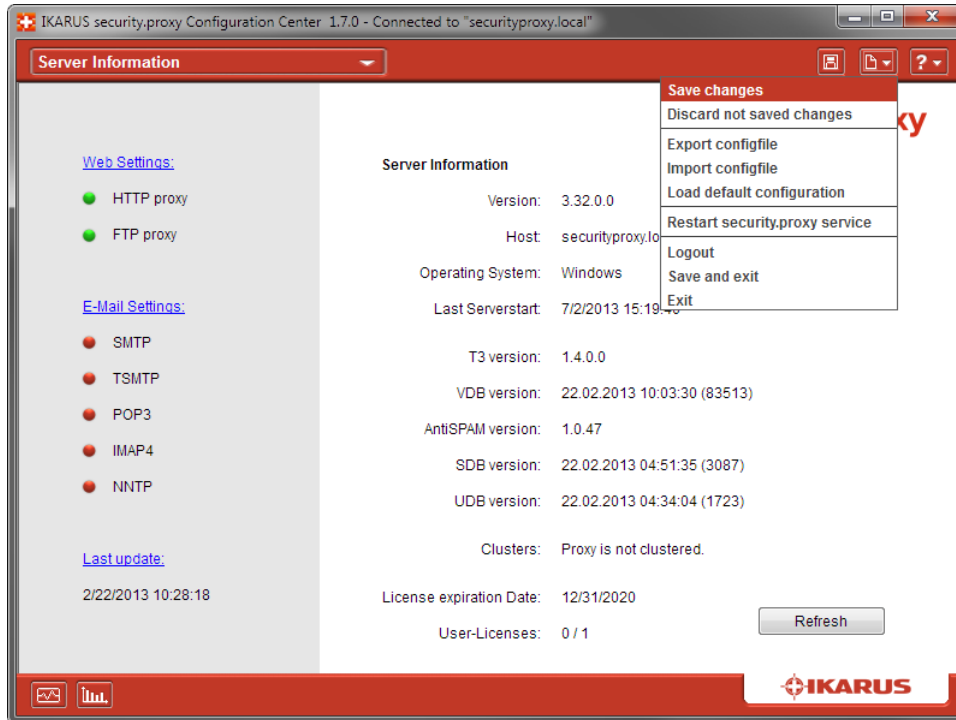


Figure 1: Edit menu



Item	Description
Save Changes	Saves all changes made to the configuration and applies them to <b>IKARUS security.proxy</b> . If applying the changes requires restarting <b>IKARUS security.proxy</b> , a dialog will be displayed.
Discard not saved changes	Discards all not saved changes and resets config to last saved status.
Export configfile	Use this option to save the current <b>IKARUS security.proxy</b> settings to a specified position as a text file.
Import configfile	Select this option to import an externally stored configuration file to <b>IKARUS security.proxy</b> .
Load default Configuration	Use this option to restore the <b>IKARUS security.proxy</b> default settings (i.e. the settings that were configured when <b>IKARUS security.proxy</b> was installed). Caution: Note that selecting this option will permanently overwrite the existing settings, so they cannot be restored.
Restart <b>IKARUS security.proxy</b> service	You can manually restart the service, for example, for applying changes to the configuration.
Logout	Use this option to log out from the <b>IKARUS security.proxy Configuration Center</b> . The <b>IKARUS security.proxy Configuration Center</b> will close, and the login screen will be displayed.
Save and exit	Saves all changes made to the configuration and applies them to <b>IKARUS security.proxy</b> . Next, <b>IKARUS security.proxy Configuration Center</b> will be terminated. If applying the changes requires restarting <b>IKARUS security.proxy</b> , a dialog will be displayed.
Exit	Use this option to quit the <b>IKARUS security.proxy Configuration Center</b> .

Table 1: Edit menu

## 3.2 Help Menu

The Help menu allows for changing global settings (e.g. the display language) of the **IKARUS security.proxy Configuration Center**, managing licenses, and storing support information.



Figure 2: Help menu

Item	Description
Language	Use this option to change the UI language of the <b>IKARUS security.proxy Configuration Center</b> . The following UI languages are available at the time of writing: English, German and Italian. When selecting the option, a dialog box where you can set the desired language is displayed. Make your settings, then click the "Apply" button to apply the changes. Changes will become effective only after a restart of the <b>IKARUS security.proxy Configuration Center</b> .
License	Clicking this item opens a dialog box where you can manage your <b>IKARUS security.proxy</b> licenses. The dialog box includes a list of all licenses that exist for the managed <b>IKARUS security.proxy</b> installation. Click the "Clean-up Licenses" button to remove expired or invalid licenses. Clicking the "Delete License" button deletes a license highlighted in the list. Using the "Add License" button allows for adding a new license.
Manual	Opens the <b>IKARUS security.proxy</b> User Manual.
Contact	Displays contact information.
Save Support Info	Clicking this item opens a dialog where you can create a support-information file. The created ZIP file contains support specific information including the configuration file, log files, license information, and version information. When you have created the file, you can send it to our customer support as necessary.
About	Opens a dialog showing the current <b>IKARUS security.proxy</b> version.
License Agreement	Opens a dialog showing the <b>IKARUS security.proxy</b> license agreement.

**Table 2:** Help menu

### 3.3 Server Information

If you have logged in successfully, a system summary will be displayed. The Server Information page has two columns. Enabled and disabled **IKARUS security.proxy** services will appear in the left column; the column on the right will display the following:



Figure 3: Server Information

Item	Description
Version	The <b>IKARUS security.proxy</b> version
Host	The name of the server host where <b>IKARUS security.proxy</b> is installed
Operating System	The operating system on the server host where <b>IKARUS security.proxy</b> is in store
Last Serverstart	The last time <b>IKARUS security.proxy</b> was started
T3 version	Shows the version of the IKARUS Scan Engine
VDB version	Shows the version of the IKARUS Virusdatabase
AntiSPAM version	Shows the version of the IKARUS Antispam Plugin
SDB version	Shows the version of the IKARUS Spam Database
UDB version	Shows the version of the IKARUS URL Database
Clusters	The cluster status
License expiration Date	Date, when the actual best license will expire
User-Licenses	If your license is limited to a certain number of users you can check here how many users are used already.
Refresh Button	Refreshes the number of currently active users.

Table 3: Server Information

### 3.4 Global Settings

Use this screen to set the global parameters of **IKARUS security.proxy**.

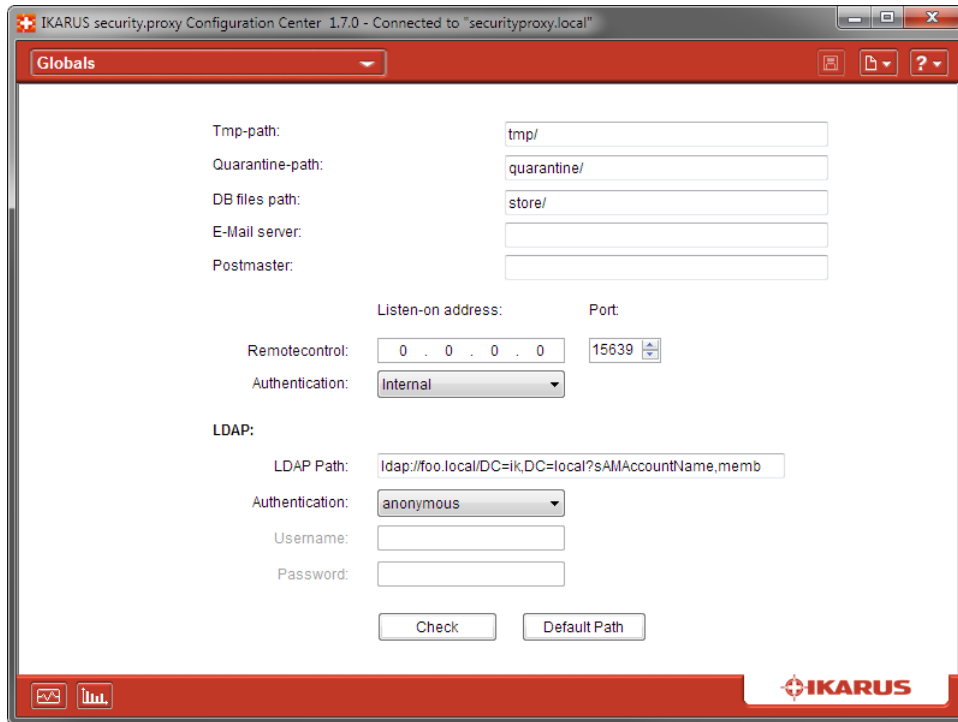


Figure 4: Global settings

Item	Description
Tmp path	Path where <b>IKARUS security.proxy</b> creates temporary files.
Quarantine path	Path where <b>IKARUS security.proxy</b> puts infected or blocked files.
DB files path	Path where the databases for Reporting and Greylisting are put in.
E-Mail server	Mail server (SMTP server) used for sending notifications such as notes, alerts, etc.
Postmaster	Address used as sender of automated e-mail.
Remote Control (Listen-on Address, Port)	Address and port where <b>IKARUS security.proxy</b> allows connections used for administering the <b>IKARUS security.proxy Configuration Center</b> . If you enter the address 0.0.0.0, you can establish connections over any available network interfaces.
Authentication	Sets the Mode how to Authenticate at Remotemanager: <ul style="list-style-type: none"> <li>• Internal: uses <b>IKARUS security.proxy</b> User-management</li> <li>• LDAP: uses Active Directory</li> </ul>

Table 4: Global settings

Item	Description
LDAP Path	Specify the LDAP path here. See below for an example.
Authentication	This setting allows for selecting between anonymous and simple authentication. When using simple authentication, specify a user name and a password.
Username	User name used for simple authentication on the LDAP server.
Password	Password used for simple authentication on the LDAP server.
Button "Default Path"	If the <b>IKARUS security.proxy Configuration Center</b> runs on a computer that is part of a Windows domain, this function allows for automatically entering the default path.
Button "Check"	Click this button to verify your configuration settings. Be sure to save the settings before using this function.

Table 5: LDAP

### Sample LDAP Path

```
ldap://dc.int.local/DC=int,DC=local?sAMAccountName,memberOf?sub?(objectClass=person)
```

dc.int.local is the internal domain controller / LDAP server

**Caution:** When using an LDAP standard connection, all data will be transferred as plain text. For configuring a secure LDAP connection with encrypted transmission, replace "ldap://" with "ldaps://" and add ":636" after the server name. (This is the port number.)

### Sample Secure LDAP Path

```
ldaps://dc.int.local:636/DC=int,DC=local?sAMAccountName,memberOf?sub?(objectClass=person)
```

## 3.5 Alerting

This item allows configuring alerts. Alerts will be triggered by specific conditions defined here. The system writes alert messages to a log file or sends notifications via e-mail.

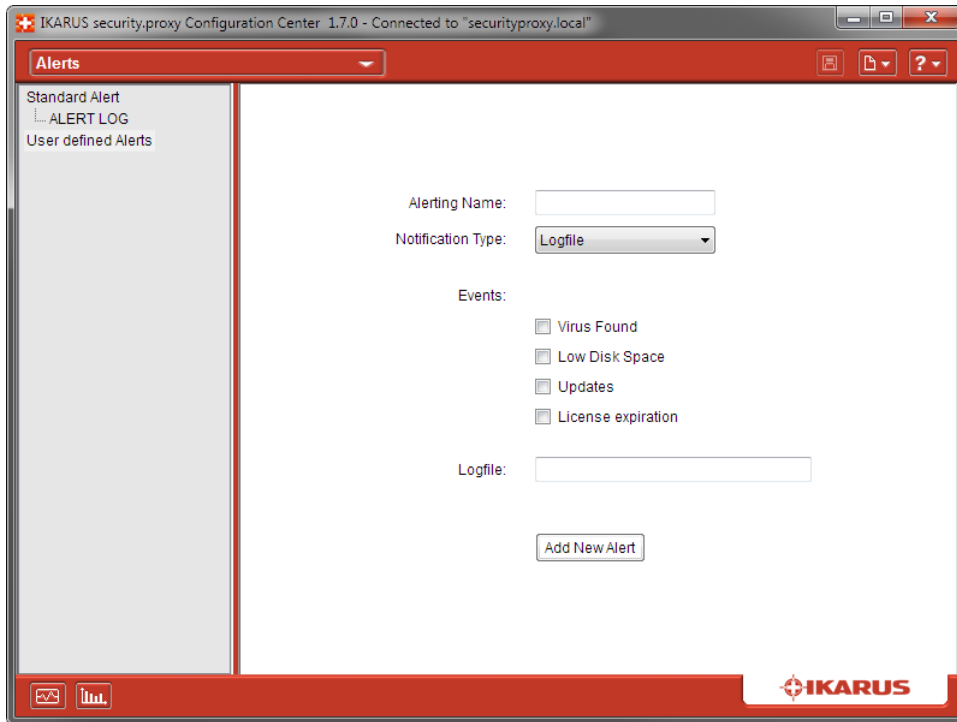


Figure 5: Alerting

Item	Description
Alerting Name	Name of the alert.
Notification Type	Selects whether the alert is written to a log file or a notification is sent via e-mail.
Events	Use this item to define the conditions that must be met to trigger an alert. Supported events include <ul style="list-style-type: none"> <li>• Virus found</li> <li>• Low disc space</li> <li>• Updates</li> <li>• License expiration (30 days, 14 days and daily starting with 12 days before expiration)</li> </ul>
Logfile/E-Mail	Depending on the selected notification type, enter the log-file path or the e-mail address to send alert notifications to.
Button "Add New Alert" / "Delete Alert"	Click this button to create a new alert with the specified settings. When selecting an existing alert, clicking this button will delete it.

Table 6: Alerting

### 3.6 Auto-Update

This item allows for configuring the auto-update feature of **IKARUS security.proxy**. Auto update ensures maximum security at any time by keeping **IKARUS security.proxy** up to date. When the feature is enabled, **IKARUS security.proxy** will automatically pull updates from the IKARUS servers every ten minutes.



Figure 6: Auto-Update

Item	Description
Active autoupdate	Checking this box enables the auto update feature.
Last Update	The last time <b>IKARUS security.proxy</b> was successfully updated.
Last Check	The last time <b>IKARUS security.proxy</b> tried to perform an auto update (regardless of whether it was successful or not).
T3 version	Shows the version of the IKARUS Scan Engine
VDB version	Shows the version of the IKARUS Virusdatabase
AntiSPAM version	Shows the version of the IKARUS AntiSPAM Plugin
SDB version	Shows the version of the IKARUS Spam Database
UDB version	Shows the version of the IKARUS URL Database
Button "Update Now"	Clicking this button starts the update process manually.

Table 7: Auto-Update



### 3.7 Logging

This is where you set the logging parameters.

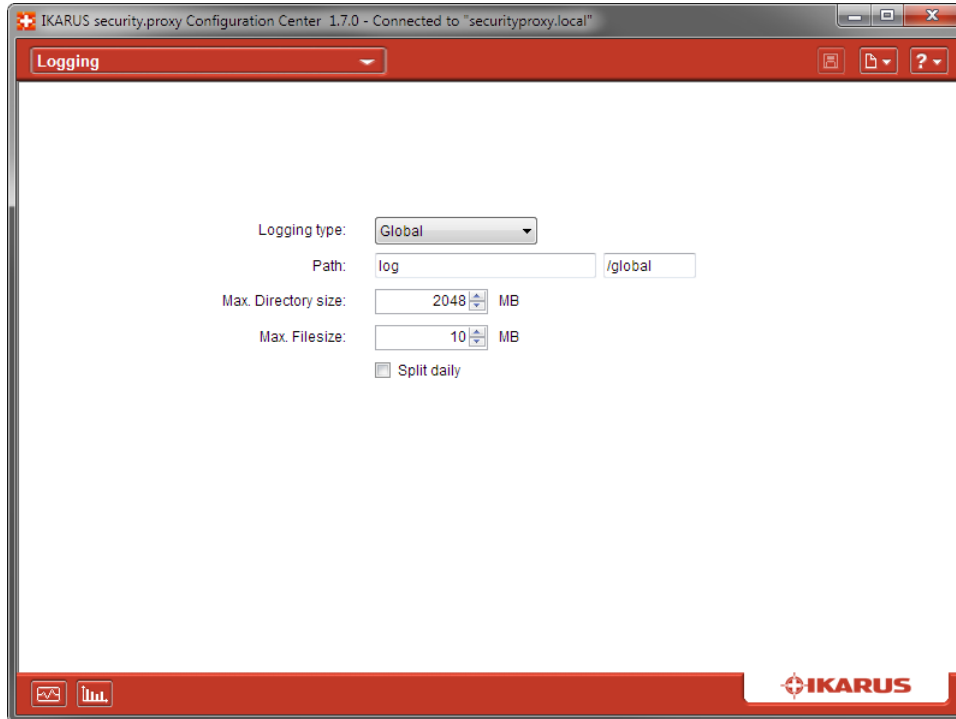


Figure 7: Logging

Item	Description
Logging type	The type of log file that the settings relate to. The following options are available: <ul style="list-style-type: none"> <li>• Global</li> <li>• Web</li> <li>• E-Mail</li> <li>• Debug</li> </ul>
Path	The path where the logfile of the selected type will be stored. The value is a path relative to the <b>IKARUS security.proxy</b> installation folder.
Max. Directory size	The maximum size of the directory used for log files of the selected type.
Max. Filesize	The maximum size of a log file.
Split daily	At the beginning of a day, the old log file will be stored and a new one will be started.

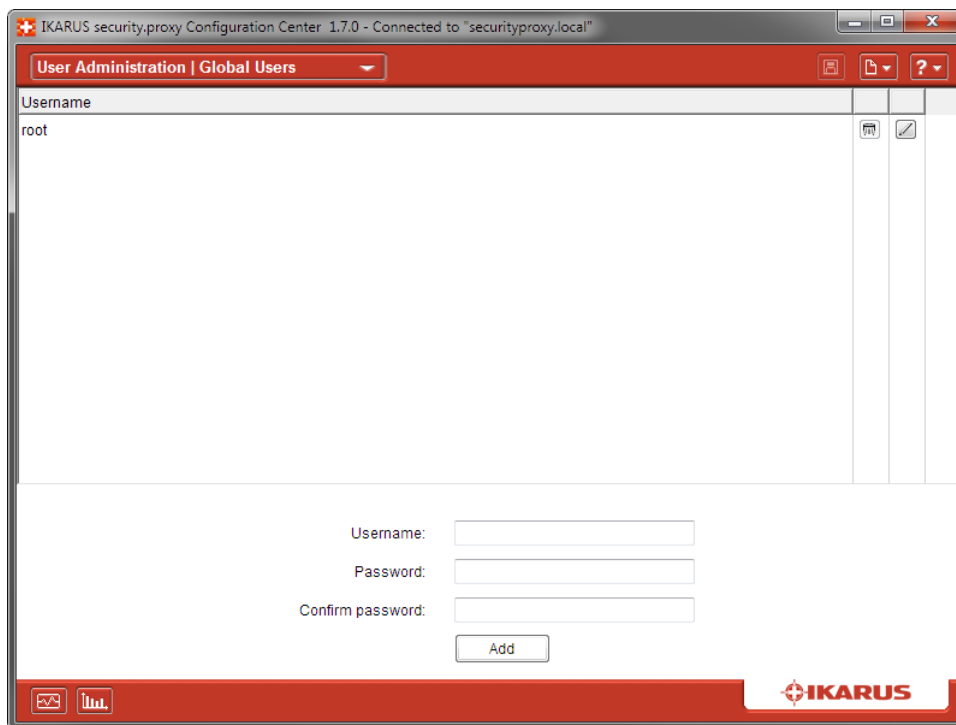
Table 8: Logging

## 3.8 User Administration

User Administration allows for configuring administrative access to **IKARUS security.proxy**.

### 3.8.1 Global Users

Users are saved within a Password-File along with their passwords – passwords are encrypted. The management is simple. Add/delete users or set/change passwords are to be done here.



**Figure 8:** Global users

### 3.8.2 Remote Manager

You can control the access based on the source IP address or the user ID.

The system provides a default admin user with the "ROOT" user ID, which cannot be removed. After reinstallation, be sure to reconfigure the password of that account.

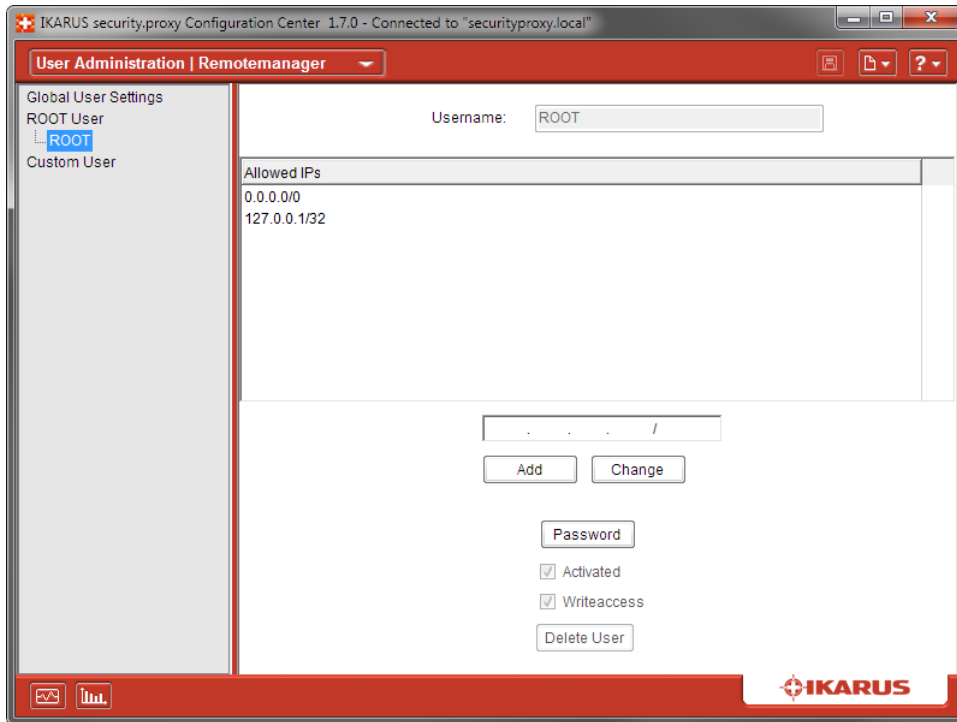


Figure 9: Remote manager

Item	Description
Global User Settings	Allows for controlling the access based on the source IP address. By default, every IP address including "localhost" may access <b>IKARUS security.proxy</b> for management purposes. If you want to perform administrative steps exclusively on the server (requires the <b>IKARUS security.proxy Configuration Center</b> and the <b>IKARUS security.proxy</b> to be installed on the same server machine running Microsoft Windows), you may configure exclusive access for "localhost".
ROOT User	Cannot be deleted. The account can be limited to specific source IP addresses. Password changes are supported.
Custom User	You can add a new user by entering the user ID and clicking the "Add" button. This account, too, can be limited to specific source IP addresses. Enable the "Write Access" permission to provide write access to the user. To delete a user, click the "Delete User" button.

Table 9: Remote manager

### 3.9 Web Settings

With **IKARUS security.proxy**, you can run an HTTP and an FTP proxy.

Web-client proxy settings also support specifying HTTPS proxies; of course, **IKARUS security.proxy** supports this approach, too. For encrypted communication, it creates a tunnel between the client and the HTTPS target server. Note that there will be no virus protection implemented on the gateway level, as this would require additional setup steps and extra software. IKARUS Security Software offers an optional HTTPS plug-in. This plug-in applet allows for checking HTTPS traffic for malware; if interested, please contact **IKARUS**.

### 3.9.1 HTTP Proxy

Use this screen to enter or edit the HTTP-proxy settings.

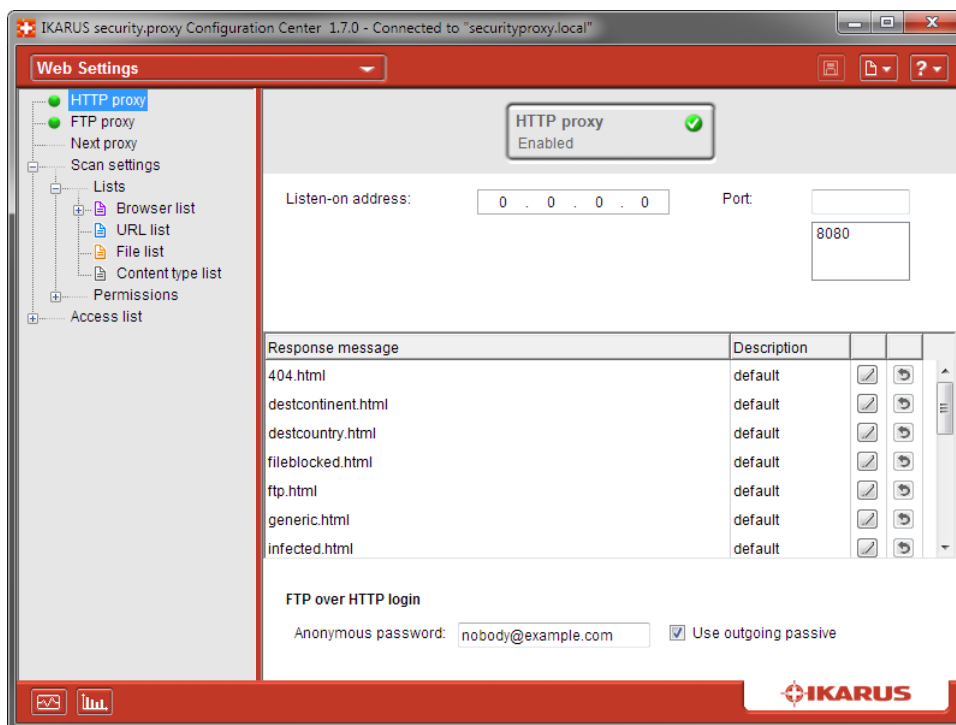


Figure 10: HTTP proxy

Item	Description
Button "HTTP proxy"	Click this button to enable or disable the HTTP proxy. Note that saving the changes is required for the changes to become effective.
Listen on address	The IP address where <b>IKARUS security.proxy</b> makes the HTTP proxy service available. Specifying the 0.0.0.0 address will cause <b>IKARUS security.proxy</b> to bind the service to all network interfaces available.
Port	The port (or multiple ports) that the HTTP proxy service runs on (by default, 8080). You can enter any other port that is not used by a different service. Note that selecting a port that is already used by a different service or program may result in conflicts.
Response message	This is a list of response pages. Response pages are HTML pages that are sent to the browser if a web page is not available (for example if it has been blocked or a page with malicious content has been found). Click the edit icon next to a list item to view the HTML code of that response page. You can change response pages to suit your needs; for that purpose, however, you need knowledge of HTML and the necessary graphics files. Therefore, if you do not need branded response pages, we recommend using the default pages.
Anonymous password	The password that is used for FTP transmission over HTTP.
Use outgoing passive	If this box is checked, <b>IKARUS security.proxy</b> uses the passive mode for FTP transmission over HTTP.

**Table 10:** HTTP proxy

### 3.9.2 FTP Proxy

**IKARUS security.proxy** also offers a proxy service for FTP. The service provides effective protection against malware transferred to your computer via FTP.

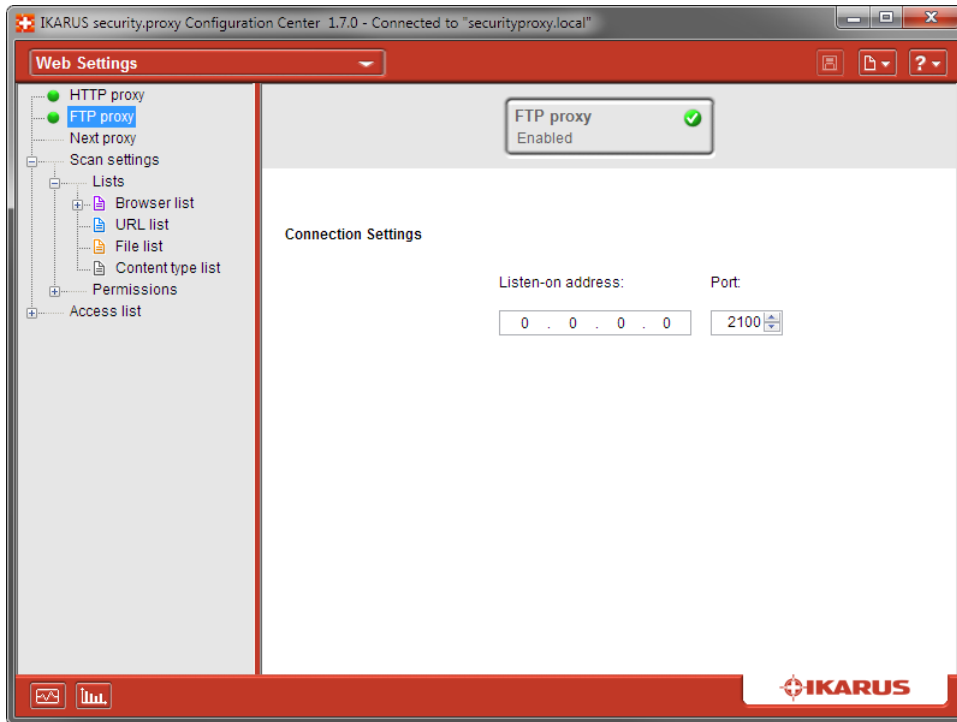


Figure 11: FTP proxy

Item	Description
Button "FTP proxy"	Click this button to enable or disable the FTP proxy. Note that saving the changes is required for the changes to become effective.
Listen on address	The IP address where <b>IKARUS security.proxy</b> makes the FTP proxy service available. Specifying the 0.0.0.0 address will cause <b>IKARUS security.proxy</b> to bind the service to all network interfaces available.
Port	The port that the FTP proxy service runs on (by default, 2100). You can enter any other port that is not used by a different service. Note that selecting a port that is already used by a different service or program may result in conflicts.

Table 11: FTP proxy

### 3.9.3 Next Proxy

You can interconnect **IKARUS security.proxy** with another proxy server. In this case, you need to provide the downstream proxy's connection parameters and credentials to allow **IKARUS security.proxy** to forward requests to that proxy.

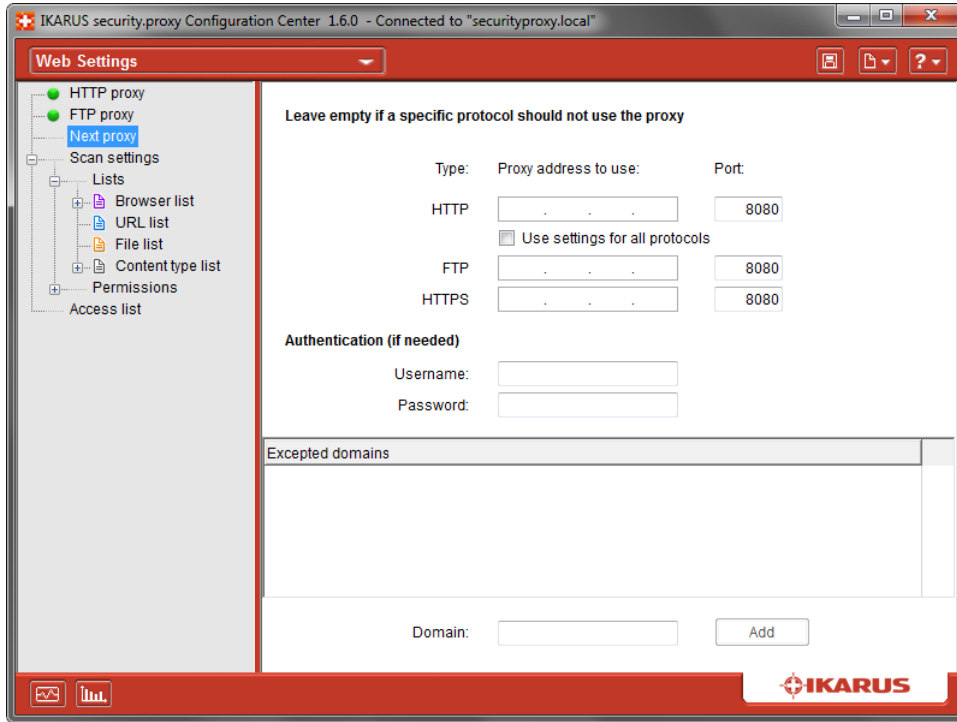


Figure 12: Next proxy

Item	Description
HTTP proxy address to use	The IP address of the downstream proxy to route HTTP requests to.
HTTP proxy Port	The port that the downstream proxy's HTTP proxy service runs on.
Use settings for all protocols	Check this box to use the HTTP proxy settings for FTP and HTTPS as well.
FTP proxy address to use	The IP address of the downstream proxy to route FTP requests to.
FTP proxy Port	The port that the downstream proxy's FTP proxy service runs on.
HTTPS proxy address to use	The IP address of the downstream proxy to route HTTPS requests to.
HTTPS proxy Port	The port that the downstream proxy's HTTPS proxy service runs on.
Username, Password	If the downstream proxy requires authentication, enter the username and password into these text boxes.
Excepted domains	This list includes all domains that will not be routed to the downstream proxy. Add a new domain by entering its name into the Domain box and clicking the Add field in the list.

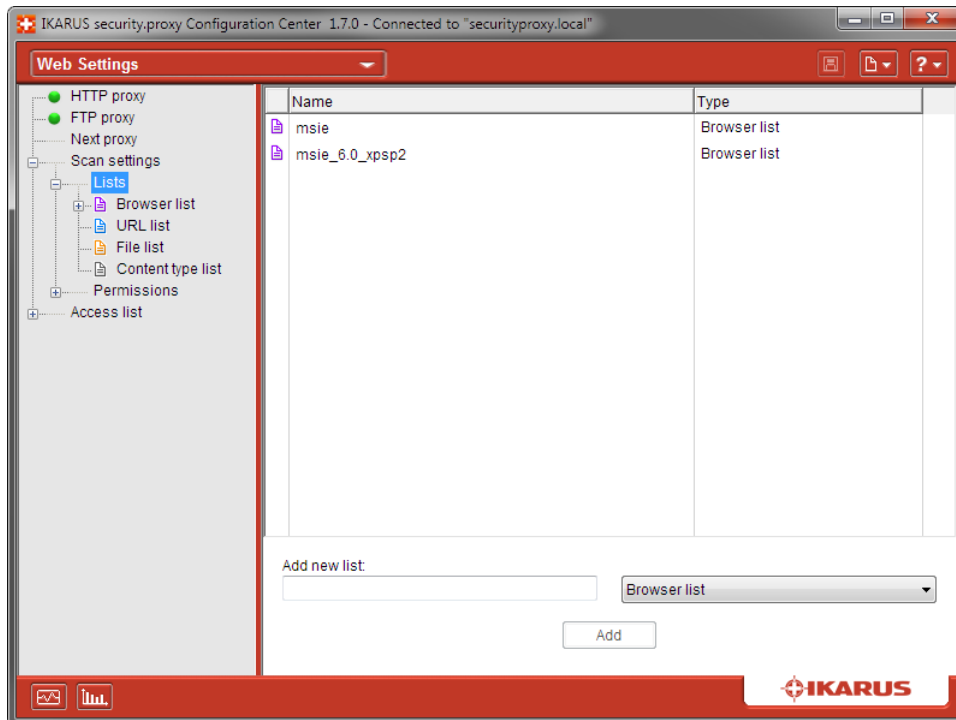
Table 12: Next proxy - proxy chain

### 3.9.4 Scan Settings

Use this screen to configure the rules applied to the HTTP proxy. For that purpose, **IKARUS security.proxy** offers many powerful configuration options.

#### Lists

- Browser List
- URL List
- File List
- Content Type List



**Figure 13:** Lists

Item	Description
Overview	Provides the name and type of the selected list.
Add new list	Enter the name of the list you wish to create.
Type	Select the type of the new list (browser list, URL list, file list, or MIME-type list) from this list box.
Button "Add"	Adds the new item to the overview. At the same time, the new list will appear in the appropriate tree-view location in the left window pane.

**Table 13:** Lists



You can add more items to a newly created list. For this purpose, select the appropriate list category in the left window pane.

### Browser list

This item allows for creating lists of web browsers. **IKARUS security.proxy** can perform browser-based filtering, for example, to allow or deny access based on the web browser used. This is beneficial if a corporate policy dictates the use of a specific browser.

**IKARUS security.proxy** implements browser-based data filtering by evaluating the user-agent string that is part of any HTTP request the client sends to the server.

For example, Internet Explorer 8.0 includes the Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64) string into HTTP requests; the user-agent string of Mozilla Firefox on a Windows OS is Mozilla/5.0 (Windows; U; Windows NT 6.1; en-GB; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13.

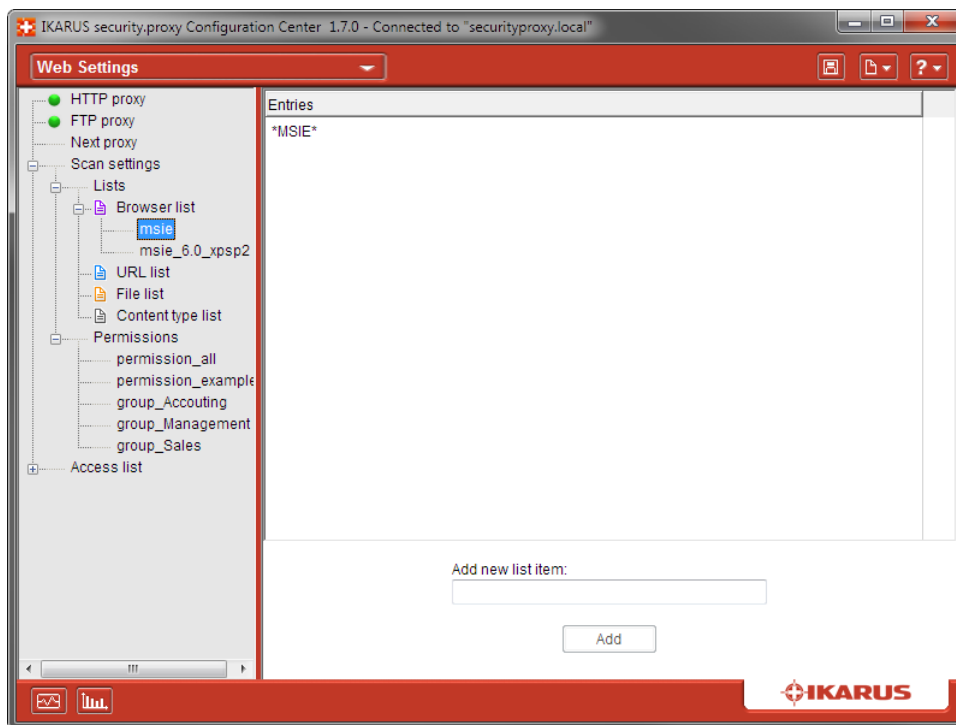


Figure 14: Sample list

You can create browser lists based on the user-agent strings. **IKARUS security.proxy** even supports wildcards for configuring the strings. The asterisk (\*) is used as wildcard character. For example, \*msie\* refers to all Internet Explorer versions.

If you do not know how to identify your browser's user-agent string, go to <http://www.useragentstring.com>. Alternatively, use a network sniffer (for example, Wireshark) for analyzing your client/server communication.

### URL list

URL lists include URLs that can subsequently be used for creating rules to allow or deny access. Be sure to

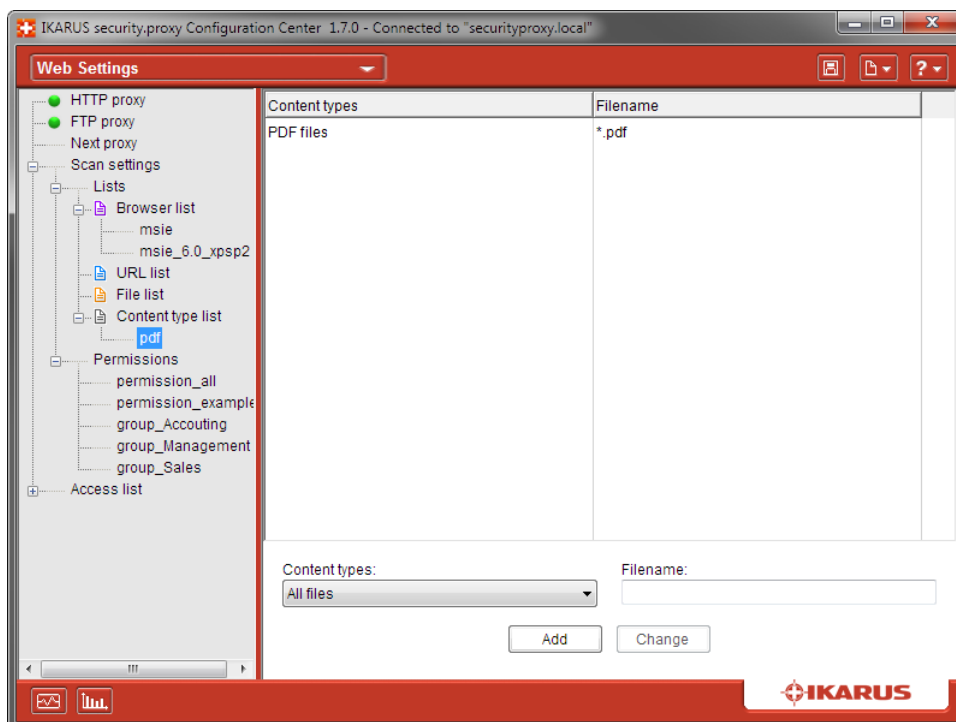
enter ASCII characters only (no spaces).

### File list

File lists allow for indicating specific file names that can subsequently be used for creating rules to allow or deny access.

You may include full file names (e.g. MyFile.doc) or use wildcards, for example, for creating rules for file types based on their extensions (e.g. \*.gif).

### Content type list



**Figure 15:** Sample content type list

Use this screen for configuring content-type lists. Compared to file lists, content-type lists are much more sophisticated when it comes to filter groups of files. Content-type lists filter by the actual file type rather than by file extension. This is more effective since the file extension does not reliably indicate the file contents; for example, an executable may have the .jpg extension although it is not a graphics file. Attackers using this approach may infiltrate your computer with malicious code.

Content-type filters remedy this situation. They filter files by their contents to reliably identify the actual file type.

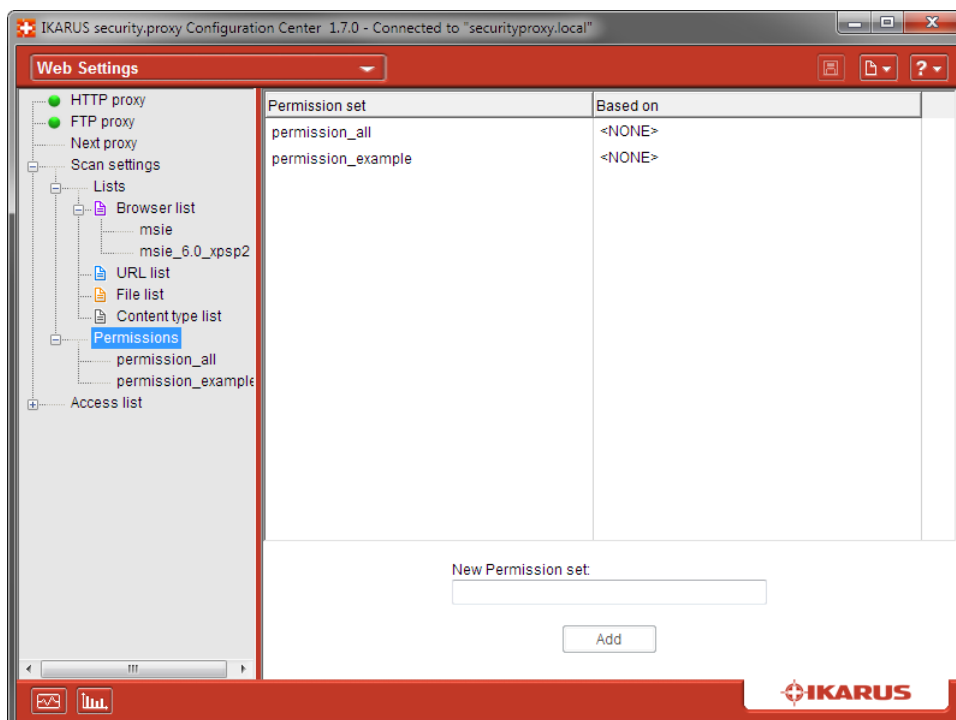
**IKARUS security.proxy** currently supports the identification of the following content types:

Content type	German name	English name
Any	Alle Dateien	All files
Archive	Archivdateien	Archive files
Executables	Ausführbare Dateien	Executable files
MS Office	Office-Dateien	Office files
Adobe Acrobat Document	PDF-Dateien	PDF files
Audio	Audio-Dateien	Audio files
Video	Video-Dateien	Video files
MS Word	Word-Dateien	Word files
MS Excel	Excel-Dateien	Excel files
MS PowerPoint	PowerPoint-Dateien	PowerPoint files
MS Visio	Visio-Dateien	Visio files

**Table 14:** Content type information

Select a content type from the Content Type dropdown box. In addition, you may enter a file name to make the filter more specific. Again, wildcards (\*) may be used. If you leave the Filename box empty, the filter will process all selected content types.

## Permissions



**Figure 16:** Permissions

Use the Permissions item for creating so-called permission sets. These are groups of filters configured using the lists. You can add any previously created lists and specify whether matching items will be allowed or denied access.

A permission set contains a list of rules which are processed according their priority. The first matching rule applies. Access will be granted or denied depending on the result.

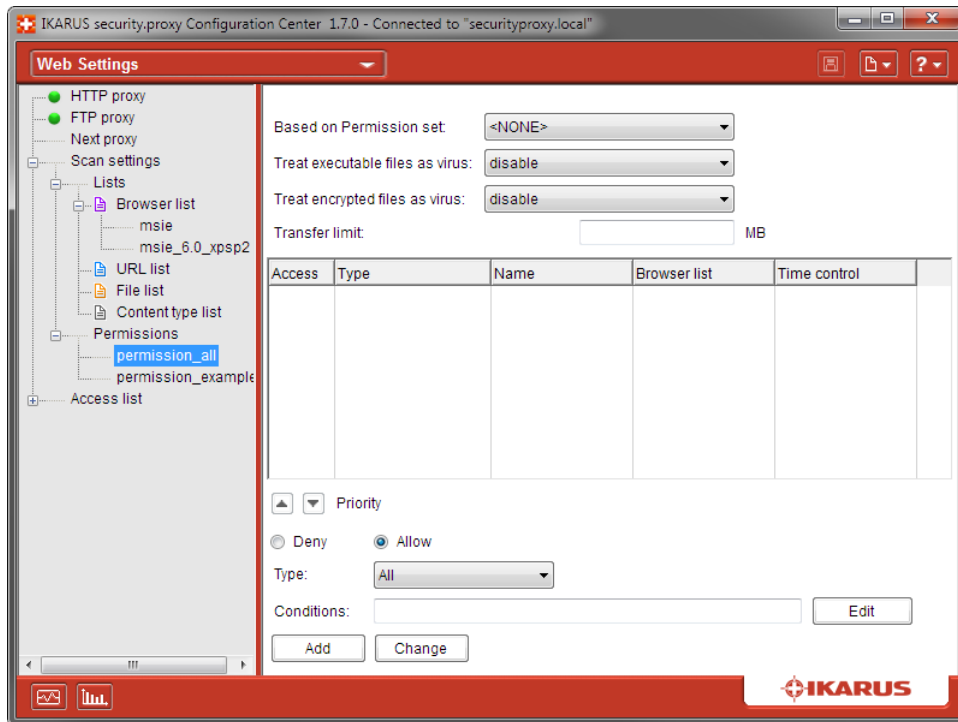


Figure 17: Permission Sets

Item	Description
Based on Permission set	Allows for referencing an existing permission set. The new set inherits the permissions of the existing permission set.
Treat executable files as virus	If this box is checked, executables will be treated as malicious software and will be deleted. If the permission set is based on another set, you may select the Inherit option to have the setting inherited.
Treat encrypted files as virus	If this box is checked, encrypted files will be treated as viruses and will be deleted. If the permission set is based on another set, you may select the Inherit option to have the setting inherited.
Transfer limit	Defines the maximum amount of data allowed.
Overview	The overview lists the rules assigned to the permission set.
Priority	Increase or decrease the priority of the selected rule.
Allow/Deny	The result for the rule.
Type	Use this dropdown box to add criteria to the rule. Depending on your selection, controls for entering the criterium value may be displayed. Options include: <ul style="list-style-type: none"> <li>• All</li> <li>• URL list</li> <li>• URL</li> <li>• Content-type list</li> <li>• Content type</li> <li>• File list</li> <li>• File/Extension</li> <li>• URLFilterCategory</li> </ul>
Conditions	Defines additional criteria for the rule. Rules are only processed if all conditions match. Options include <b>Browser list</b> , <b>Time control by weekday</b> , and <b>Time control by time of day</b> .
Button "Add"	Adds the newly created rule to the permission set.
Button "Change"	Updates the selected rule.

**Table 15:** Permissions

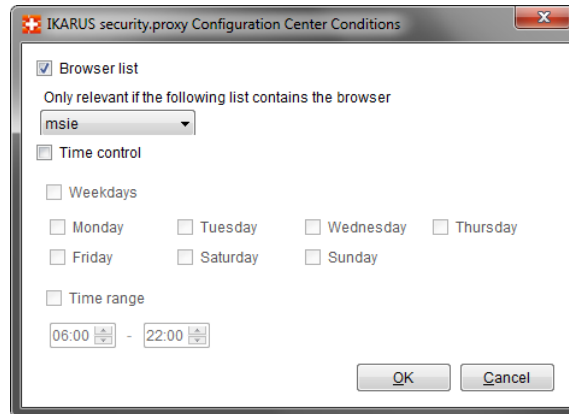


Figure 18: Conditions for permission sets

## URL Filter Categories

The URL filter is another powerful tool of **IKARUS security.proxy**. It provides categorization of URLs by subject (e.g. adult, e-commerce, malware, games, etc.) based on default rules. Numerous URLs have already been assigned to each category. By adding a category to a permission set, you can allow or deny the access to all of the URLs in that category. IKARUS Security Software periodically updates the URL lists. Therefore, using URL filters is a safe and convenient way of denying access to inappropriate websites.

### 3.9.5 Access List

Access lists allow for assigning permission sets to IP addresses or subnets and for enabling them. In addition, you can set the authentication method to be used.

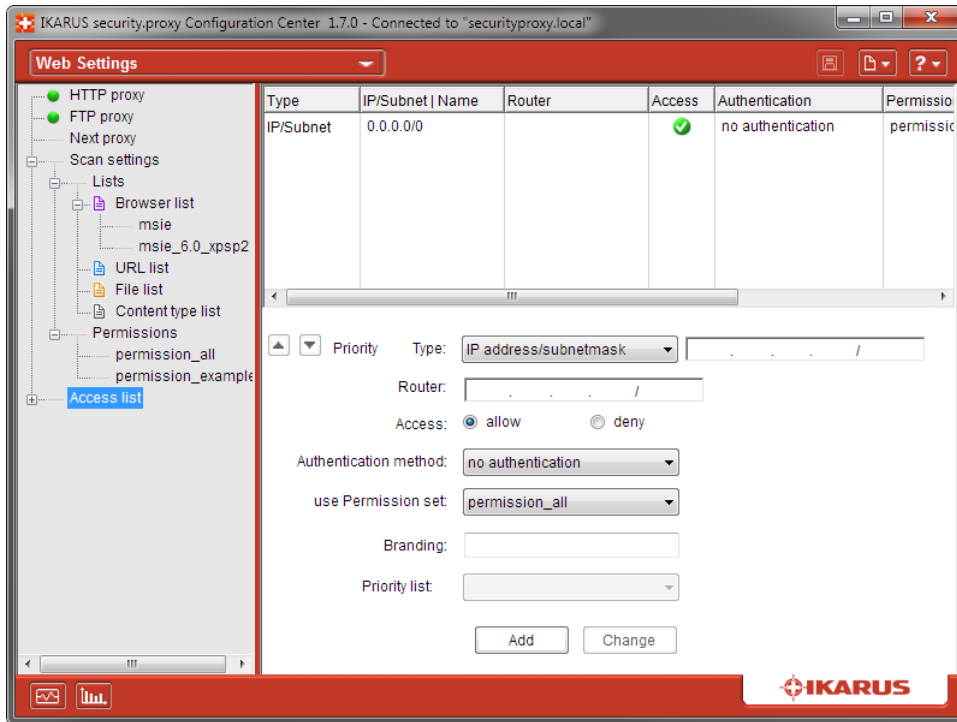


Figure 19: Access list

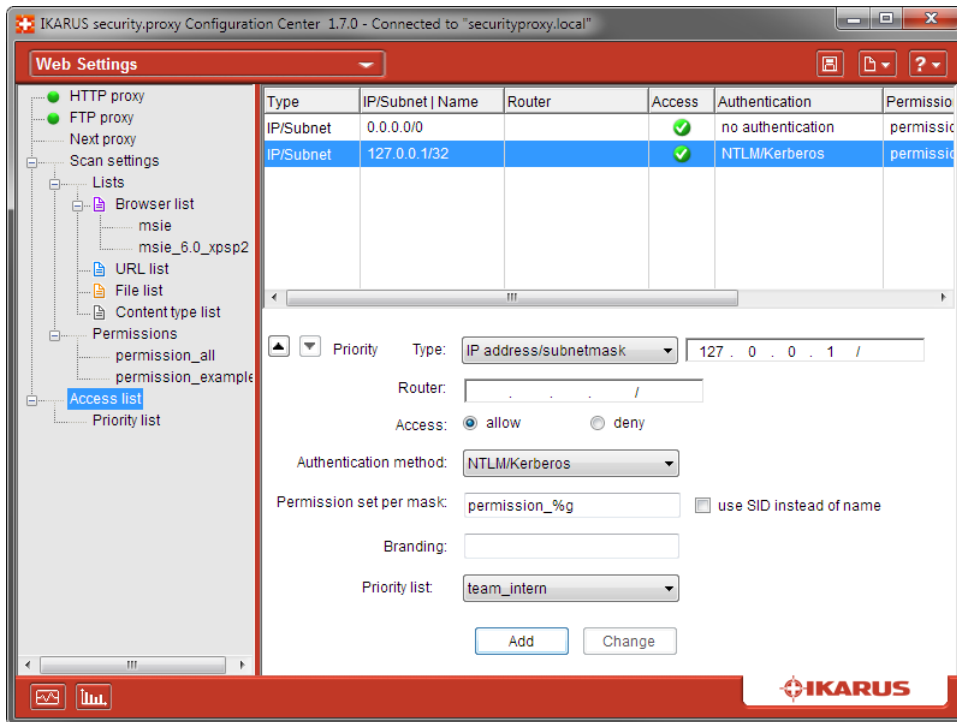


Figure 20: NTLM/Kerberos

Item	Description
Overview	This list includes individual target IP addresses or subnets plus information on whether access is allowed or denied, the selected authentication method, and the permission set applied.
Priority	Allows to increase or decrease the priority of a (previously selected) item in the overview.
Router	IP address of GRE router used for the IP addresses or subnets.
Type	Allows for specifying an IP address or a network.
Access	Allows or denies access for an entry.
Authentication mode	The type of authentication to be used for the selected network or IP address. Options include: <ul style="list-style-type: none"> <li>• no authentication</li> <li>• proxy internal authentication</li> <li>• LDAP authentication</li> <li>• NTLM/Kerberos (only works on Windows)</li> </ul>
Use Permission set	Adds a Permission set to the item.
Permission set per mask	Chooses with a mask, which permission sets are used for this access list. Valid placeholders are %u and %g and at least one must be used. For further information see 4.6.8.
Use SID instead of name	When replacing the placeholders in the permission set mask, SIDs are used instead of group and user names.
Branding	Defines the branding to be applied for the selected network (see 4.3.2).
Priority list	Defines the list that should be taken to determine the order of groups in case the groups of a user match multiple permission sets.
Button "Add"	Adds the newly created entry to the overview.
Button "Change"	Updates the selected entry in the overview.

**Table 16:** Access list

### Priority list

In this window priority lists can be added and deleted, as well as entries in the lists can be modified. Depending on using SIDs or names, according entries must be added. Those lists are used to determine the first permission set that should be used if a multiple groups of a user match multiple permission sets. To increase or decrease the priority of an entry, it can be moved up and down with the arrows.



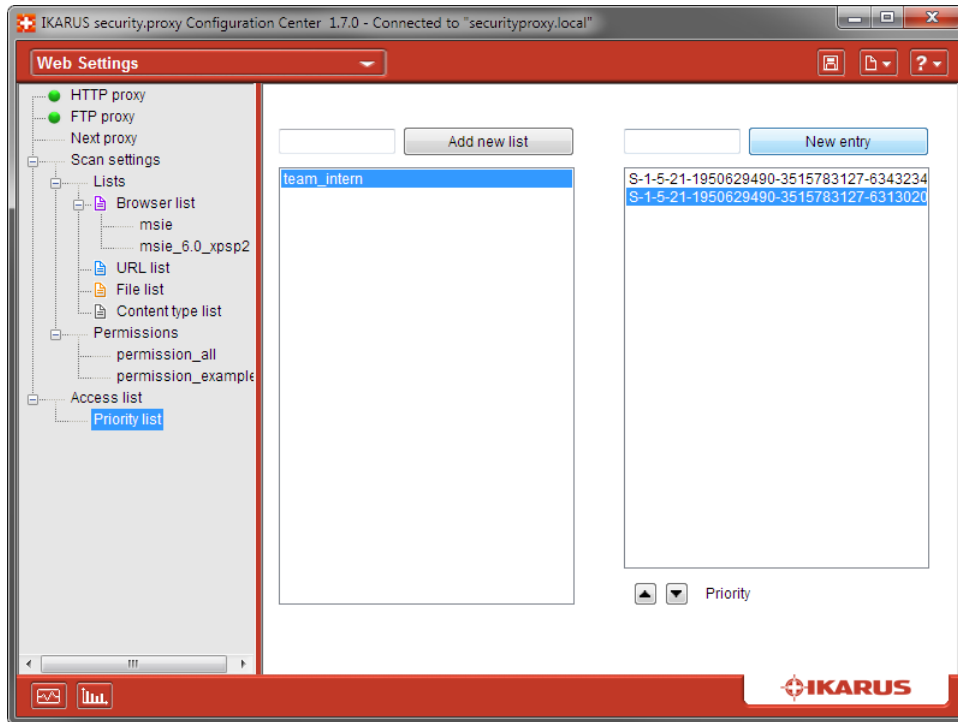


Figure 21: Priority list

### 3.10 Mail Settings

In the E-Mail Settings all protocols which can be scanned are listed. The scan rules can be set for each protocol separately.

### 3.10.1 Scan Rules

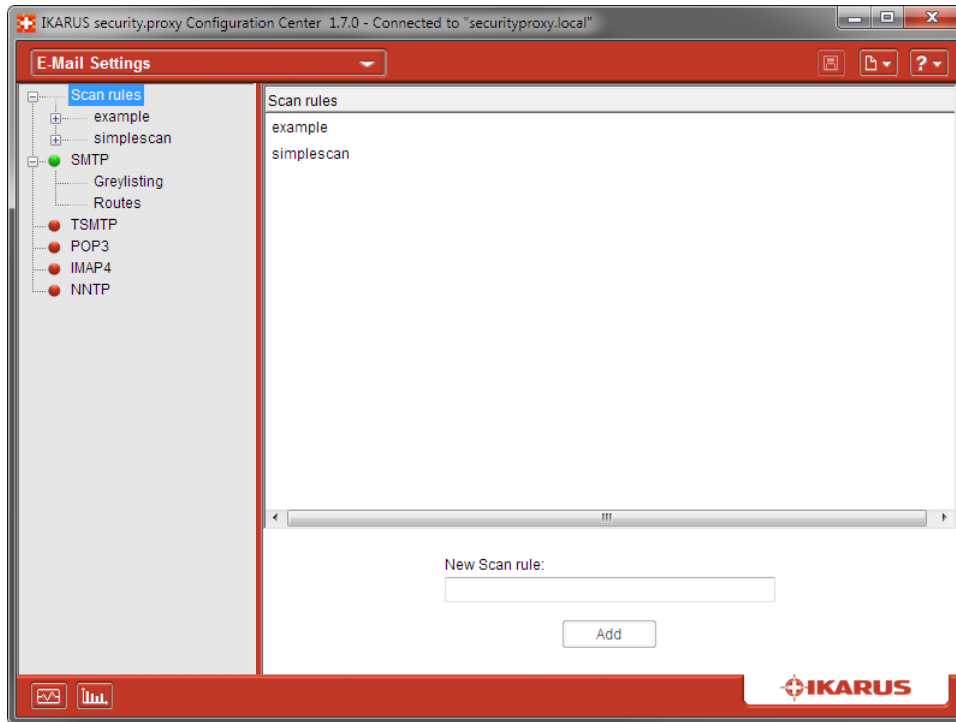
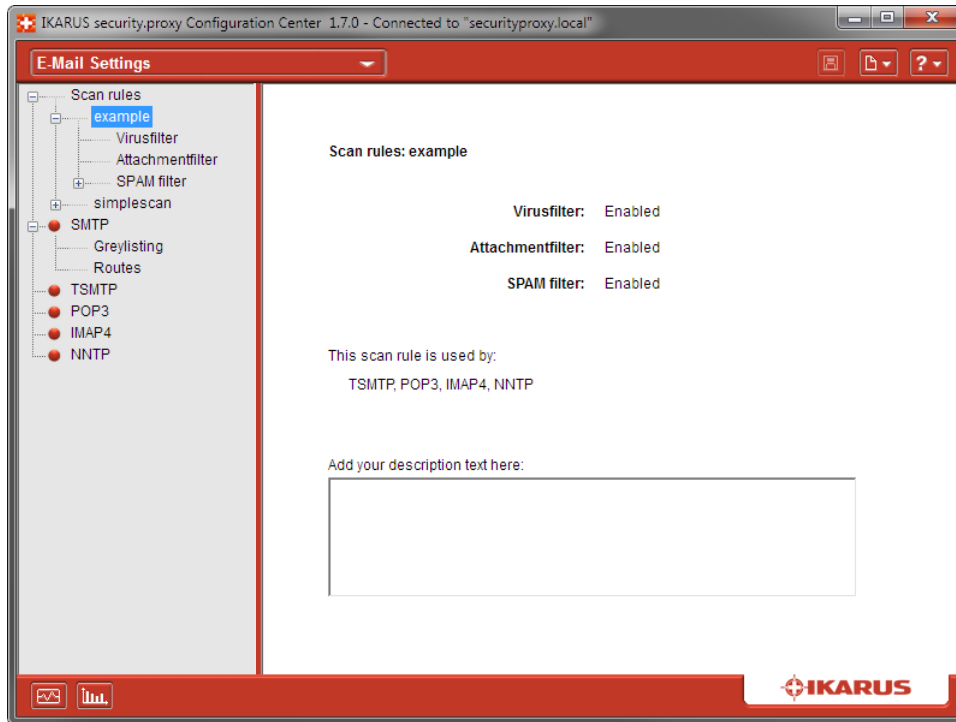


Figure 22: Scan rules overview

To ensure effective protection, **IKARUS security.proxy** allows for specifying custom scan rules. You can create separate rules for SPAM, e-mail attachments, and malware. Custom rules are applicable to the following protocols:

- SMTP
- TSMTP
- POP3
- IMAP4
- NNTP

You can create an unlimited number of rule sets. In addition, different rule sets can be defined for the various protocols. The SMTP functions of **IKARUS security.proxy** even allow for applying rules to individual routes.



**Figure 23:** Sample scan rule

## Creating Rules

To configure a rule, you first need to create it. Enter a rule name. The name can consist of any alphanumeric characters plus hyphens, underscores, and periods. Scan rules you have added will appear in the tree view on the left. To edit the rule you have just created, click its name in the tree view. Various settings are available for the following features:

- Virus filter
- Attachment filter
- SPAM filter
- SPAM rules

## Virus filter

The virus-scanner settings are the most significant rules. This is where you enable or disable the virus scanner and configure its behavior.

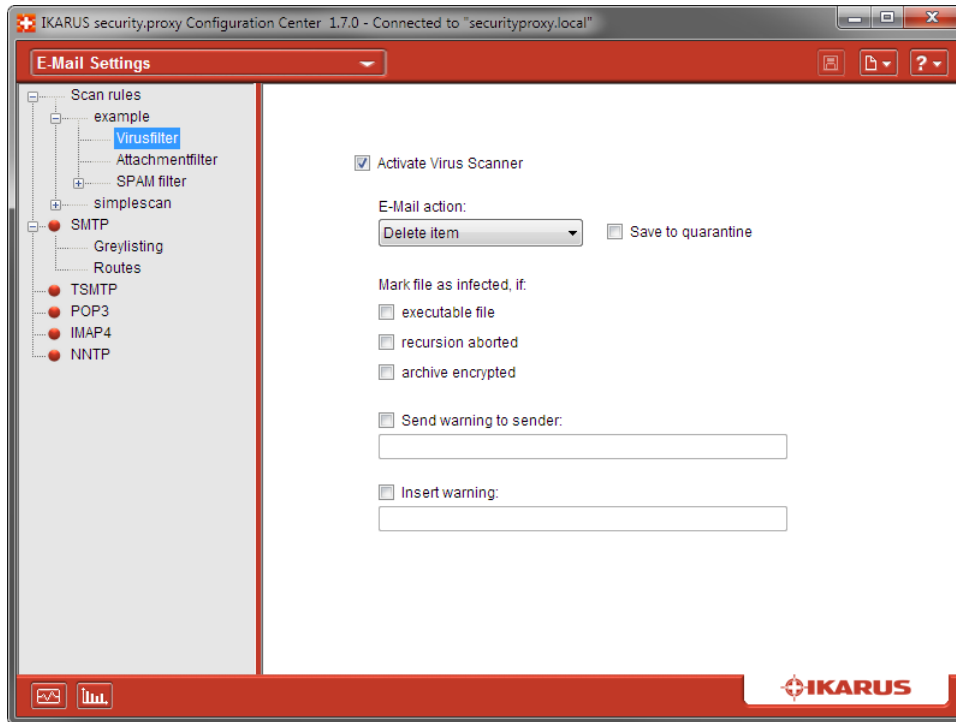


Figure 24: Virus filter

Item	Description
Activate Virus Filter	Check this box to enable the virus filter, or clear it for disabling.
E-Mail Action	Determines the action to be performed when a virus has been found. Options include "Delete Item" and "Drop E-Mail". Selecting the first option will delete the attachment only; otherwise, the entire message will be deleted.
Save to quarantine	When this option is enabled, the blocked files will be stored to the server's quarantine directory.
Mark file as infected, if	
executable file	If the file is executable it will be blocked.
recursion aborted	When a specific recursion depth is reached while unpacking the files, they will be handled like infected files (i.e. blocked).
archive encrypted	Scanned archives that are encrypted will be blocked.
Send warning to sender	When this option is enabled, the scanner will send a notification to the sender of the message. Enter the desired notification text into the text box.
Insert warning	Inserts a warning text into the message if a virus has been found. Enter the desired warning text into the text box.

Table 17: Virus filter

### Attachment Filter

The attachment filter allows for setting up rules for executables.

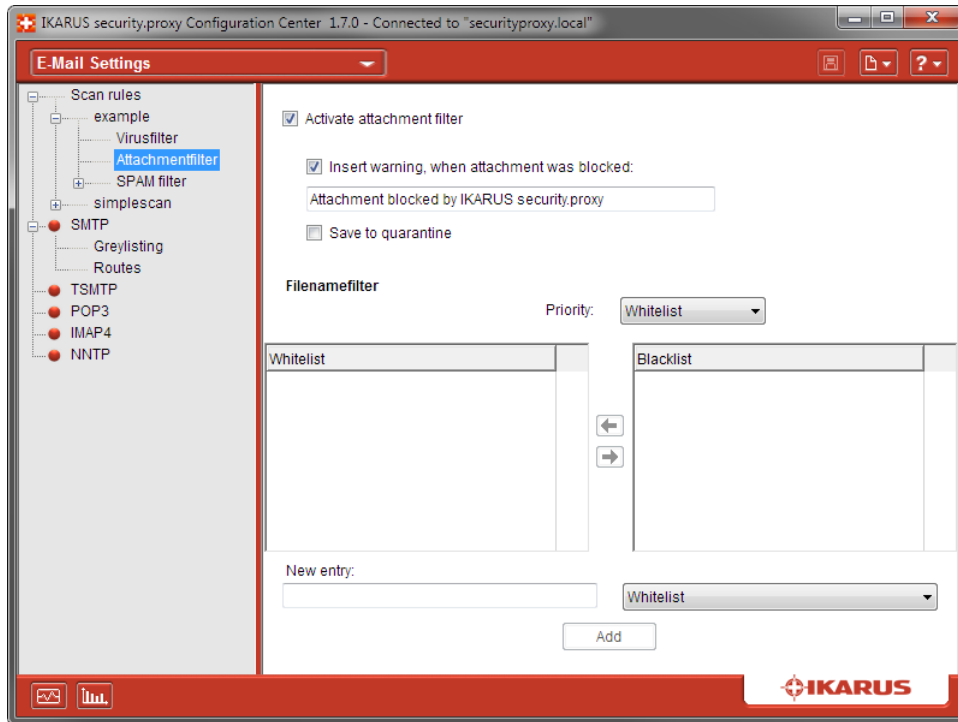


Figure 25: Attachment filter

Item	Description
Activate attachmentfilter	Check this box to enable the attachment filter, or clear it for disabling.
Insert warning, when attachment was blocked	The text entered here will be inserted into messages if an attached executable has been deleted.
Save to quarantine	When this option is enabled, blocked executables will be stored to the server's quarantine directory.

Table 18: Attachment filter

### Filename filter

The filename filter allows you to set up blacklists and whitelists. Using this filter, you can configure that e-mail with specific file attachments will always be delivered or blocked, respectively. When adding a new entry, you first need to select whether it will be added to the blacklist or the whitelist. In addition, you need to select which of the two lists will be processed first using prioritization. The list with the higher priority overrides the other one.

### SPAM filter

IKARUS security.proxy also includes a highly effective SPAM filter. You can adjust thresholds to identify messages that may be SPAM, and those, that are definitely SPAM, and configure how to handle those messages.

IKARUS security.proxy provides default rules for SPAM filtering. Therefore, to establish effective SPAM protection, you just need to enable the filter and configure how to deal with SPAM.

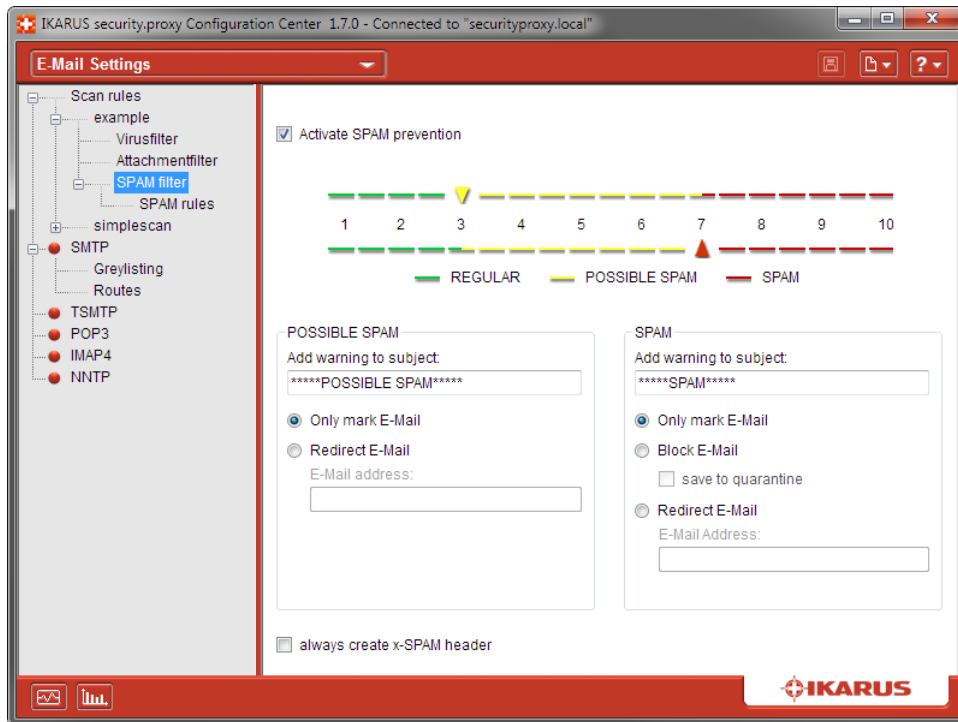


Figure 26: SPAM filter

Item	Description
Activate SPAM prevention	Check this box to enable the SPAM filter, or clear it for disabling.
SPAM Slider	Use this slider to configure thresholds for possible and definite SPAM. The SPAM filter assigns a score to each incoming e-mail message. Messages receive score points for specific features typical of SPAM (e.g. if message includes the string "V1@gR@"). The higher the score of an e-mail, the more probable it is that it is a SPAM message. By configuring the thresholds, you define when a message is suspicious of being SPAM, and when it is definitely considered SPAM. Note that lower thresholds increase the possibility of false positives (i.e. legitimate messages falsely been identified as SPAM). Similarly, too high threshold values may lead to SPAM not being identified correctly.
Possible SPAM	
Add warning to subject	Allows for configuring text that is added to the subject line of the e-mail message.
Only mark E-Mail	Messages classified as possible SPAM will be marked accordingly.
Redirect E-Mail	Messages classified as possible SPAM will be redirected to the e-mail address specified below. Note that this feature is supported for SMTP only.
SPAM	
Add warning to subject	Allows for configuring text that is added to the subject line of the e-mail message.
Only mark E-Mail	Messages classified as SPAM will be marked accordingly.
Block E-Mail	A message that has been identified as SPAM will be blocked (i.e. it will not be delivered). Note that this feature is supported for SMTP only.
Redirect E-Mail	A message that has been identified as SPAM will be redirected to a previously specified e-mail address. Note that this feature is supported for SMTP only.
always create x-SPAM header	When this option is checked, <b>IKARUS security.proxy</b> will always enter an x-SPAM header into the message header.

Table 19: SPAM filter

### SPAM rules

You can define custom SPAM rules in addition to the default rules. **IKARUS security.proxy** offers a large number of options you can use for creating your rules. This rules allow for overriding filter actions performed by **IKARUS security.proxy**. For example, you can have e-mail by specific senders always marked as SPAM – even if **IKARUS security.proxy** would have been classified it as legitimate mail.

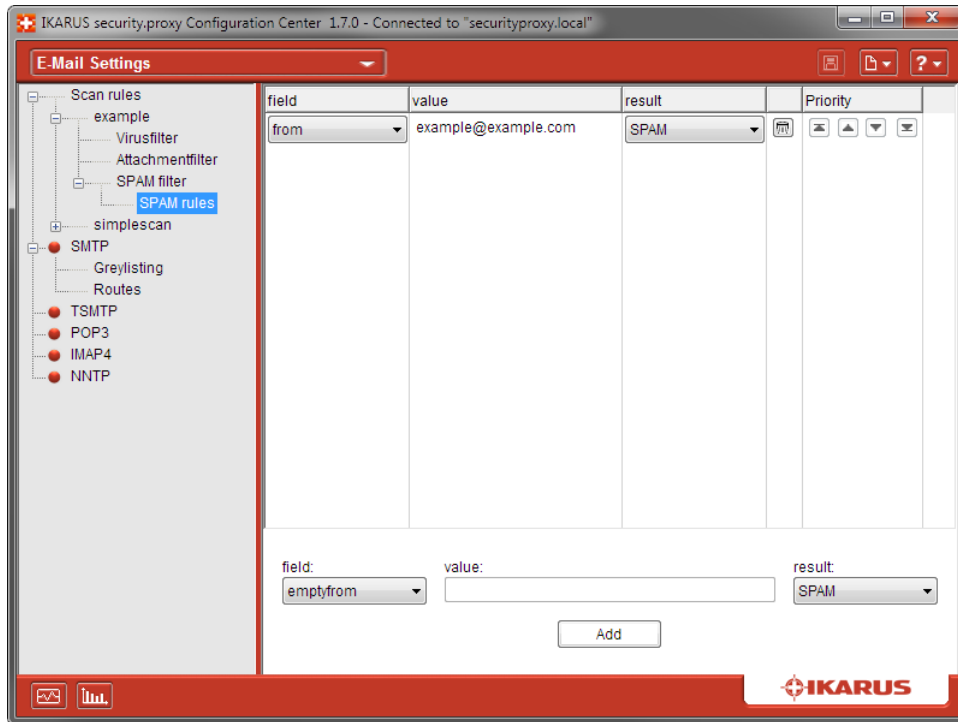


Figure 27: SPAM rules

Item	Description
fields	Specifies the part of the message that you want to create a rule for. Refer to the Fields table for details.
value	Depending on the selected message field, you can choose a specific field value. If this value matches the respective field value, the message is considered a positive.
result	Select whether a positive e-mail message is considered SPAM, possible SPAM, or a legitimate message.
Button "Add"	Adds the manually configured rule at the top of the list (i.e. with highest priority).

Table 20: SPAM rules



Field	Description
emptyfrom	Empty From header item
emptysubject	Empty Subject header item
emptyto	Empty To header item
envelope:from	SMTP envelope sender is <FROM>
envelope:to	SMTP envelope sender is <TO>
from	From header item includes <FROM>
mail:text	The e-mail body includes <TEXT>
nofromline	From header item does not exist
nosubjectline	Subject header item does not exist
notoline	To header item does not exist
novalidaddrfrom	From header item includes an invalid e-mail address
novalidaddrto	To header item includes an invalid e-mail address
onlyhtmltext	The e-mail body contains HTML code only
subject	Subject header item includes <SUBJECT>
to	To header item includes <TO>
toandfromequal	To and From header items are the same

**Table 21:** "field" values for SPAM rules

You can mark each of these rules using one of the following methods:

Item	Description
SPAM	Messages matching this rule will always be marked as "spam".
POSSIBLE	Messages matching this rule will always be marked as "possible spam".
REGULAR	Messages matching this rule will always be marked as "ham" (i.e. legitimate e-mail).

**Table 22:** SPAM classification results

If a message matches multiple contradictory rules (for example, one rule categorizes it as SPAM while another one marks it as REGULAR), prioritization will be used. That is, the rule with the higher list position will apply.

### 3.10.2 SMTP

You can run an SMTP server using **IKARUS security.proxy**. For that purpose, you need to define routes specifying how an SMTP connection is routed based on its origin. This feature allows for using **IKARUS security.proxy** for SMTP traffic on your network in numerous ways.

In addition, **IKARUS security.proxy** can check any e-mail sent via SMTP for malicious contents (for example, viruses) and filter out SPAM.

## SMTP setup

Use the E-mail Settings item in the **IKARUS security.proxy Configuration Center** to access the SMTP setup screen. Select the SMTP item from the tree view.

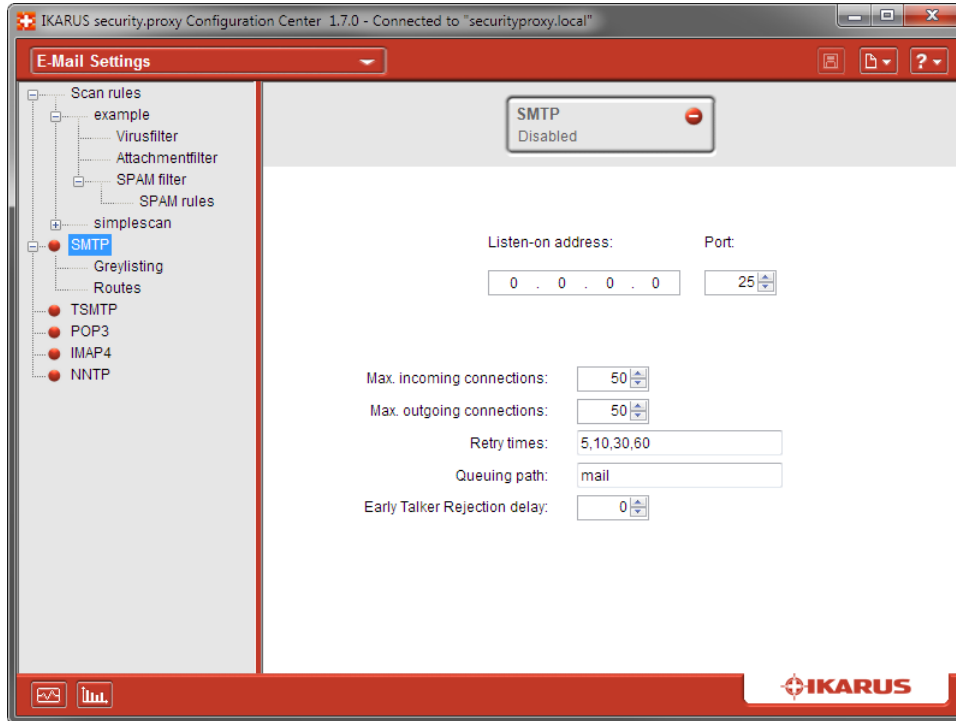


Figure 28: SMTP

Item	Description
Button "SMTP"	Click this button to enable or disable the SMTP service of <b>IKARUS security.proxy</b> . Note that saving is required for the changes to become effective.
Listen on address	The IP address of the SMTP service. Specifying the 0.0.0.0 address will cause <b>IKARUS security.proxy</b> to bind the service to all network interfaces available.
Port	The port that the SMTP service runs on (by default, 25).
Max. incoming connections	The maximum number of concurrent incoming SMTP connections supported by <b>IKARUS security.proxy</b> . When the number of connections specified here is exceeded, the proxy will send error messages to the surplus connections.
Max. outgoing connections	The maximum number of concurrent outgoing SMTP connections made by <b>IKARUS security.proxy</b> when sending e-mail.
Retry times	Sets the number and intervals of delivery retries if delivery has failed. For example, using a setting of "5, 10, 30, 60" means that the first delivery retry will be attempted after 5 minutes; the second one after 10 minutes; the third one after 30 minutes; and the fourth one after 60 minutes.
Queuing path	Path to where e-mail is queued. The setting is a path relative to the <b>IKARUS security.proxy</b> installation folder.
Early Talker Rejection delay	The number of seconds that the SMTP service waits before sending the SMTP banner. With this feature, SPAM bots can be blocked that send data in a non-compliant way, without waiting for the banner that signals the server being ready.

Table 23: SMTP

## Greylisting

The greylisting feature supports the reduction of delivered SPAM mail.

For more details on greylisting, refer to section 4.7.

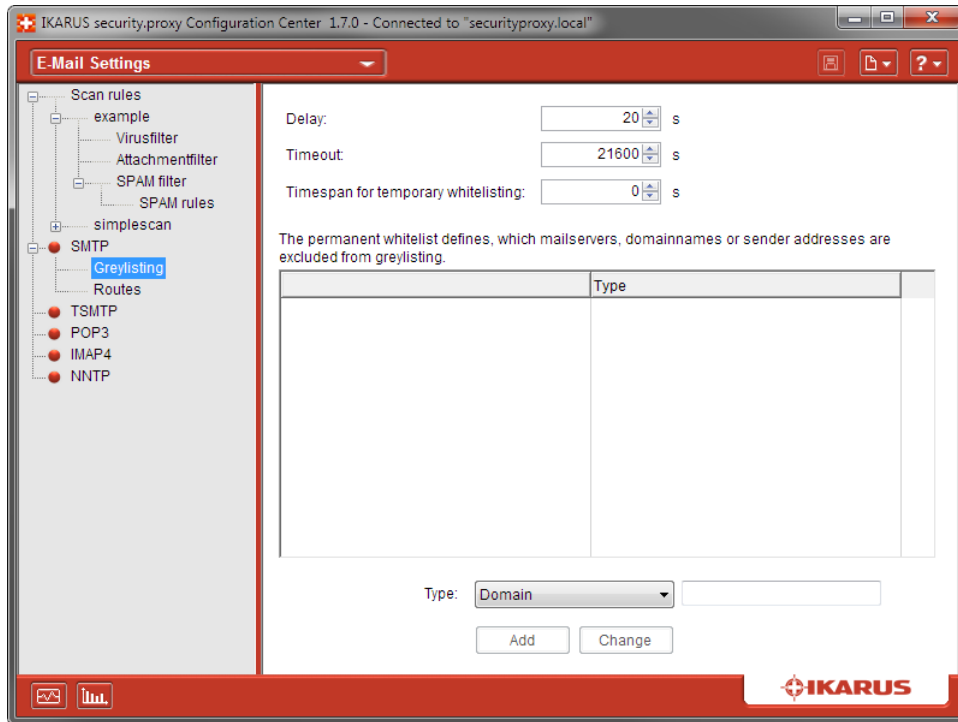


Figure 29: Greylisting

Item	Description
Delay	Minimum time frame after which a greylisted message will be accepted.
Timeout	Maximum time frame after which a greylisted message will not be accepted anymore.
Timespan for temporary whitelisting	If this parameter is set to a value greater than zero, temporary whitelisting is enabled. Addresses added to this list remain on it for the timespan defined here. After this period of time has expired, connections from this address will be subjected to the greylisting check again.
Permanent whitelist	This configurable list includes mail-server IP addresses, domain names, and e-mail addresses that the greylisting function will ignore.

Table 24: Greylisting

### Defining Routes

When running an SMTP server, you need to define routes; otherwise, **IKARUS security.proxy** cannot process incoming SMTP connections properly. You can have as many routes as needed. The rules created for the routes are included in a rule list with the highest-priority rules positioned at the top of the list. **IKARUS security.proxy** processes the list top-down.

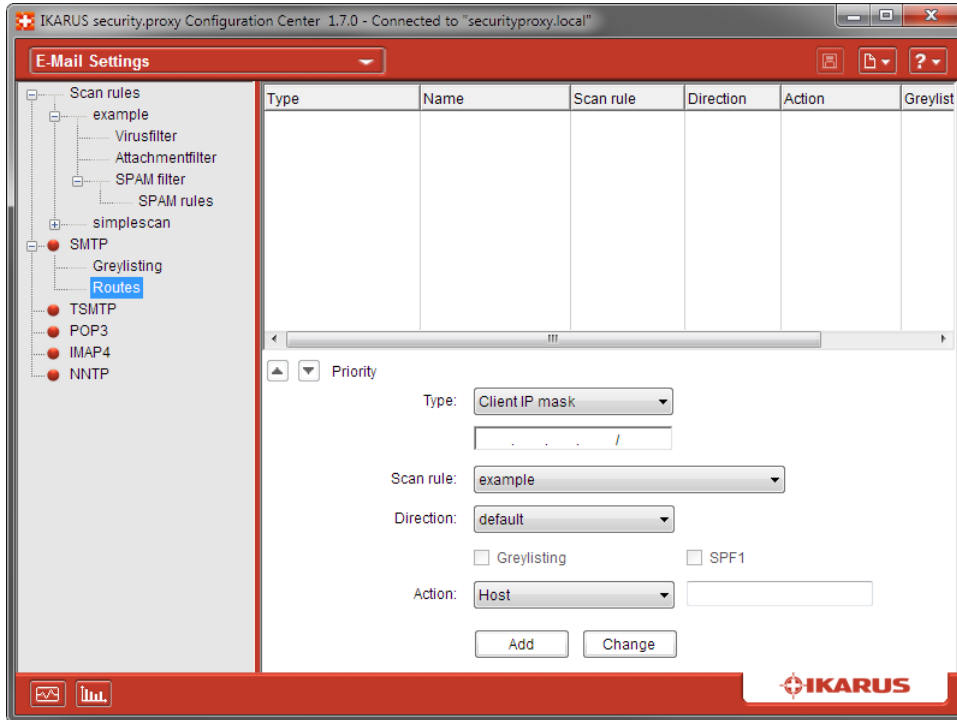


Figure 30: Routes

Item	Description
Type	Sets the route type. Routes can be based on the sender's IP address (or the IP address of the originating network), a list of target domains or target email addresses, LDAP* or a mailbox file.
Scan Rules	The scan rule to be applied must be indicated for each route.
Direction	Makes a Route inbound, outbound or standard (bi-directional).
Greylisting	For an inbound Route Greylisting can be activated.
SPF	For an inbound Route SPF can be activated.
Action	Determines how e-mail is routed. Settings include "Host" (allows for specifying either the target-host IP address or a resolvable computer name) and "MX" (tries do deliver the message to the default mail exchanger based on the receiver indicated in the SMTP envelope).

Table 25: Routes

\* By using LDAP, only mailboxes defined in the Active Directory are used for a certain route. The LDAP string must conform to the following format:

```
ldap[s]://<user-cn/dc>:<password>@<domain controller>/<query>
```

Here is an example for a valid LDAP strings for "readonlyuser@test.local" with the password "mypassword" on the domain controller "dc.test.local":

```
ldaps://CN=readonlyuser,CN=Users,dc=test,dc=local:mypassword@dc.test.local/DC=test,DC=local?proxyaddresses?sub?(proxyaddresses=SMTP:*)
```

### 3.10.3 TSMTP - the transparent SMTP Proxy

In addition to the SMTP functionality provided by **IKARUS security.proxy**, you can also use an SMTP proxy. In this case, **IKARUS security.proxy** does not store e-mail but forwards all data exchanged between the client and the SMTP server. E-mail received in that way can still be checked for viruses or SPAM.

Linux allows for running the SMTP proxy in the fully transparent mode. Provided your routes and iptables have been properly configured, this mode allows for scanning e-mail with no need for specific mailclient setup.

The transparent mode is not available for Windows OS at the moment. Instead, you can specify a default SMTP target server that the SMTP traffic received by the proxy is routed to.

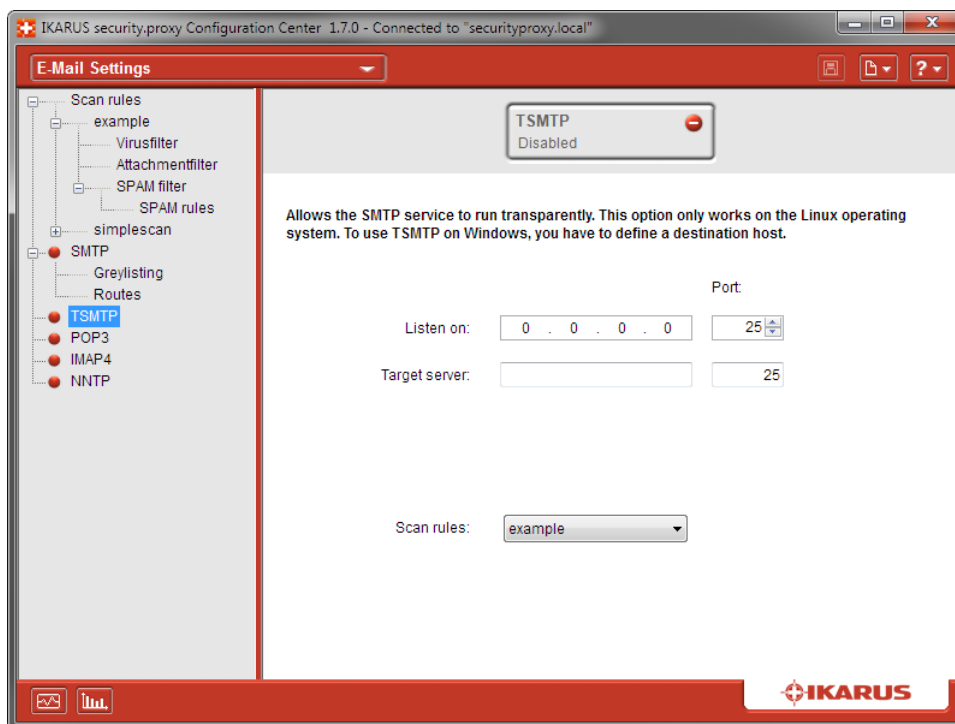


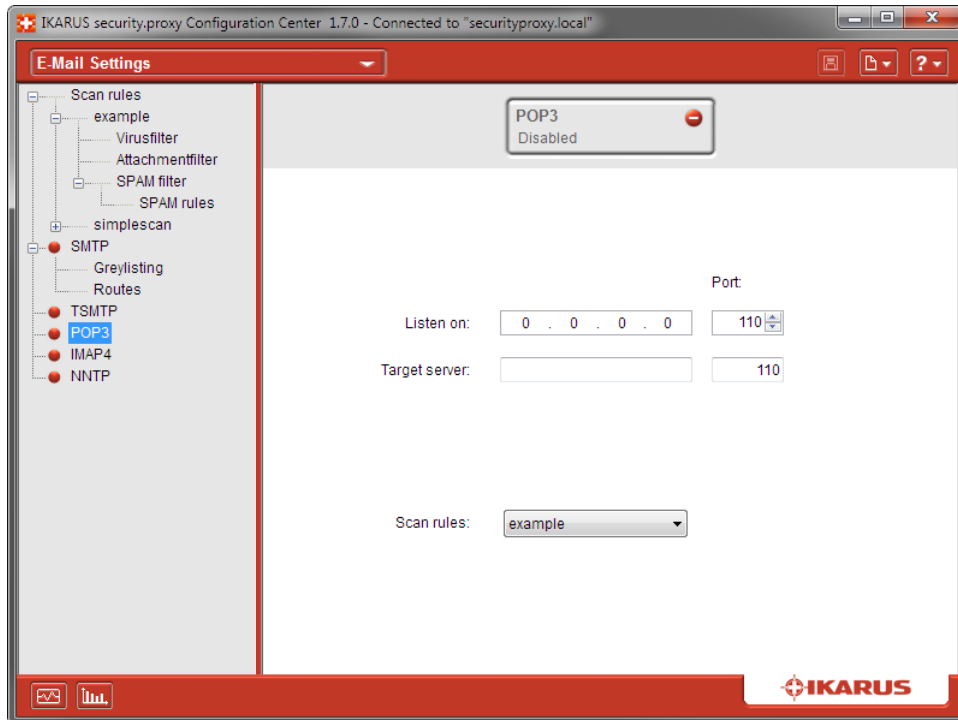
Figure 31: TSMTP

Item	Description
Button "TSMTP"	Click this button to enable or disable the TSMTP service of <b>IKARUS security.proxy</b> . Note that saving is required for the changes to become effective.
Listen on address	The IP address where the TSMTP service is run. Specifying the 0.0.0.0 address will cause <b>IKARUS security.proxy</b> to bind the service to all network interfaces available.
Port	The port that the TSMTP service runs on (by default, 25).
Target server and Port	Alternative TSMTP server. Will be used when the user name does not include a TSMTP server.
Scan Rules	Scan rule to be applied for TSMTP.

**Table 26:** TSMTP settings

### 3.10.4 POP3 proxy

You can run a POP3 proxy using **IKARUS security.proxy**. This allows for proxying unencrypted POP3 traffic. For example, you can check messages locally requested by clients from Internet-based POP3 servers for viruses and/or SPAM.



**Figure 32:** POP3

Item	Description
Button "POP3"	Click this button to enable or disable the POP3 proxy of <b>IKARUS security.proxy</b> . Note that saving is required for the changes to become effective.
Listen on address	The IP address of the POP3 proxy. Specifying the 0.0.0.0 address will cause <b>IKARUS security.proxy</b> to bind the service to all network interfaces available.
Listen on port	Port that the POP3 proxy listens on (by default, 110).
Target Server and Port	Alternative POP3 server. Will be used when the user name does not include a POP3 server.
Scan Rules	Scan rules to be applied by the POP3 proxy.

**Table 27:** POP3 settings

### How to Configure E-mail Clients

If you want to use the POP3 proxy with your e-mail clients, you need to change the configuration settings accordingly.

**POP3 server:** Enter the IP address or DNS name of **IKARUS security.proxy** instead of the POP3 server parameters to ensure the e-mail server contacts **IKARUS security.proxy** for POP3 requests.

**User name:** Add an @ sign and the computer name or IP address of the POP3 server to the user name of the POP3 mailbox.

**Example:** You have the e-mail address john.doe@example.com. The mailbox of that address has the username "john" on the POP3 server at pop.example.com. Now, if you want **IKARUS security.proxy** to receive e-mail from that POP3 server, change the username from "john" to john@pop.example.com.

Alternatively, define a default server in **IKARUS security.proxy** to forward POP3 requests to. In this case, you do not need to change the mail-account settings as described above; however, be aware that the POP3 proxy service will be limited to that POP3 server in this case.

#### 3.10.5 IMAP4 Proxy

You can run an IMAP4 proxy using **IKARUS security.proxy**. This allows for proxying unencrypted IMAP4 traffic. For example, you can check messages locally requested by clients from internet-based IMAP4 servers for viruses and/or SPAM.



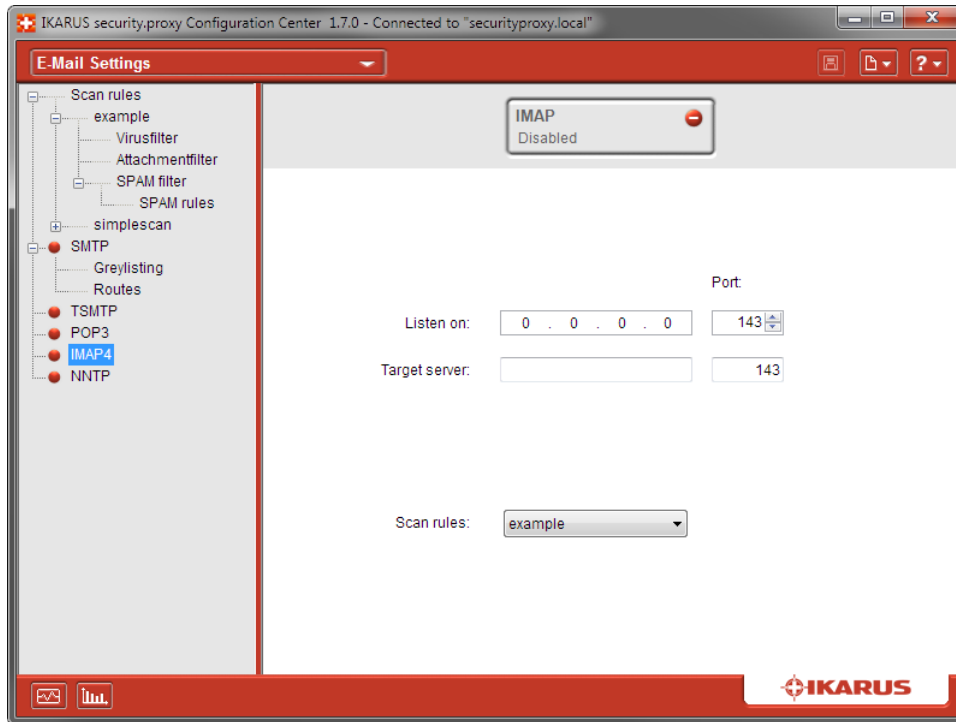


Figure 33: IMAP4

Item	Description
Button "IMAP"	Click this button to enable or disable the IMAP4 proxy of <b>IKARUS security.proxy</b> . Note that saving is required for the changes to become effective.
Listen on address	The IP address of the IMAP4 proxy. Specifying the 0.0.0.0 address will cause <b>IKARUS security.proxy</b> to bind the service to all network interfaces available.
Listen on port	Port that the IMAP4 proxy listens on (by default, 143).
Target Server + Port	Alternative IMAP4 server. Will be used when the user name does not include an IMAP4 server.
Scan Rules	Scan rules to be applied by the IMAP4 proxy.

Table 28: IMAP settings

### How to Configure E-mail Clients

If you want to use the IMAP4 proxy with your e-mail clients, you need to change the configuration settings accordingly.

IMAP server: Enter the IP address or DNS name of **IKARUS security.proxy** instead of the IMAP4-server parameters to ensure the e-mail server contacts **IKARUS security.proxy** for IMAP4 requests.

User name: Add an @ sign and the computer name or IP address of the IMAP4 server to the specified user name.

Example: You have the e-mail address john.doe@example.com. The mailbox of that address has the user-name "john" on the IMAP4 server at imap.example.com. Now, if you want **IKARUS security.proxy** to receive e-mail from that IMAP4 server, change the username from "john" to john@imap.example.com.

### 3.10.6 NNTP Proxy

In addition to mail protocols (SMTP, POP3, IMAP), **IKARUS security.proxy** also transmits the Network News Transfer Protocol (NNTP). Create and apply scanning rules for NNTP just like for any mail protocol.

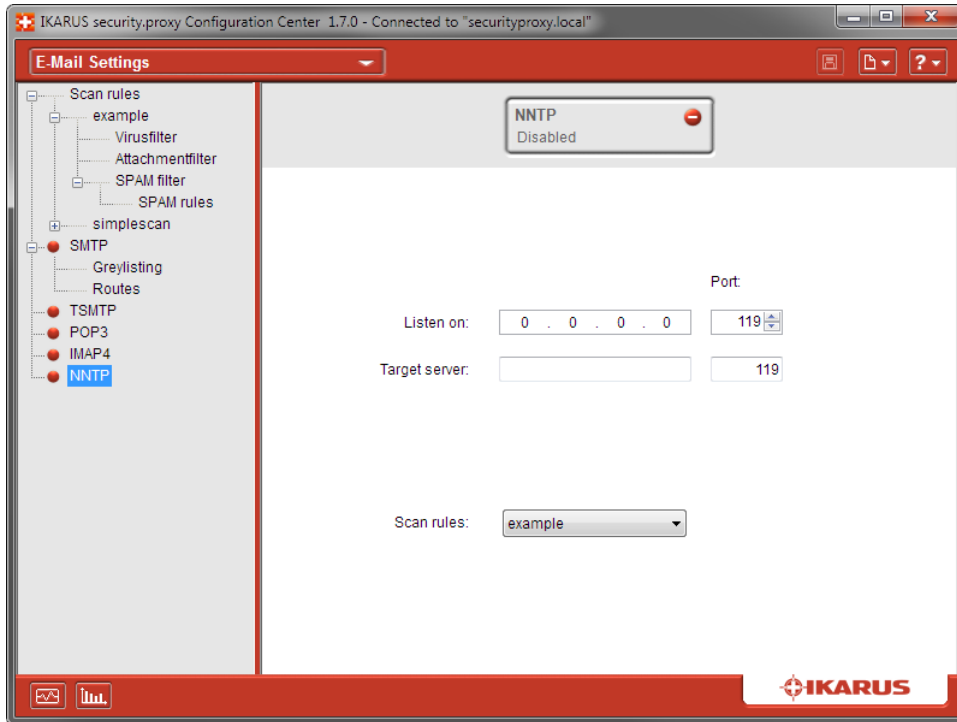


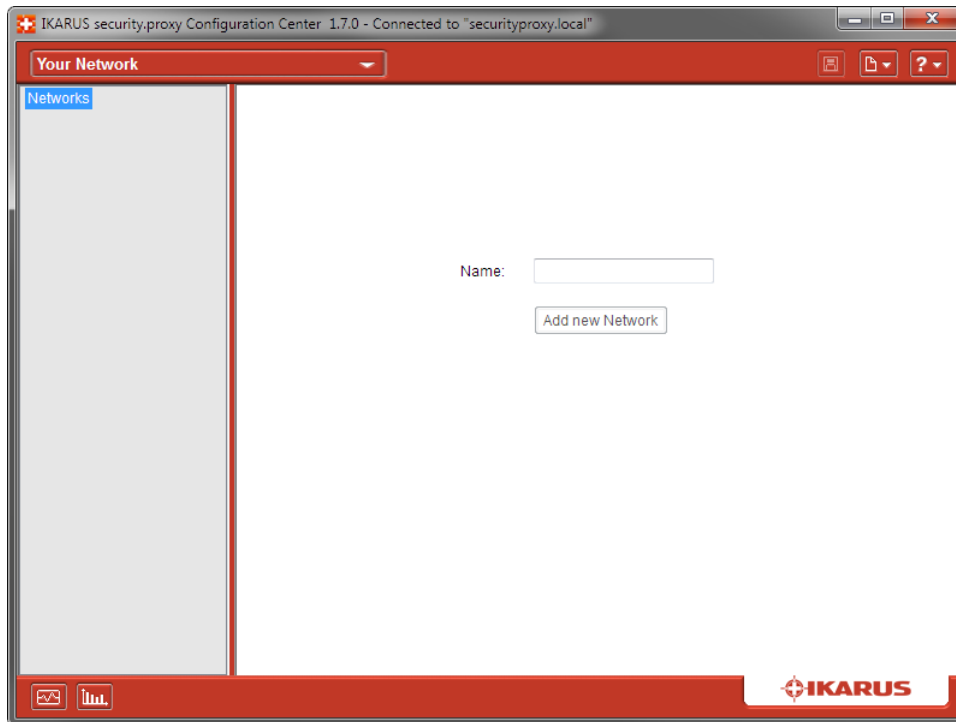
Figure 34: NNTP

Item	Description
Button "NNTP"	Click this button to enable or disable the NNTP proxy of <b>IKARUS security.proxy</b> . Note that saving is required for the changes to become effective.
Listen on address	The IP address of the NNTP proxy. Specifying the 0.0.0.0 address will cause <b>IKARUS security.proxy</b> to bind the service to all network interfaces available.
Listen on port	Port that the NNTP proxy listens on (by default, 119).
Target Server + Port	Alternative NNTP server. Will be used when the user name does not include an NNTP server.
Scan Rules	Scan rules to be applied by the NNTP proxy.

Table 29: NNTP settings

### 3.11 Your Network

**IKARUS security.proxy** supports the definition of networks. Logical groups containing the addresses of individual computers or entire networks can be defined. Use these groups as a basis for defining proxy settings.



**Figure 35:** Your Network settings

Item	Description
Name	Network name. Permitted characters include all alphanumerical characters plus hyphens ("-"), underscores ("_"), and periods (".")
IP address/IP mask	IPv4 address and the corresponding subnet mask. Individual IP addresses are defined by choosing /32 (32 host bits, no network bits) as a subnet mask.
Button "Add new Network"	Click this to add names to the configured network.
Button "Delete Network"	Click this to delete the selected network name. Note that a name cannot be deleted when it is part of an access list.

**Table 30:** Your Network settings

### 3.12 Clustering

You can create a cluster made up of multiple **IKARUS security.proxy** instances. Doing so will keep the configuration settings of all instances in sync. Note that a cluster must include at least two **IKARUS security.proxy** instances; however, it is not important on which OS the proxy instances involved are running. For example, creating a cluster containing Windows and Linux proxies at the same time is possible.

Note that entering the IP address of the local proxy is required in order to create a cluster. When using the cluster functionality the default port for the remote manager (port 15639) must not be changed. Otherwise the sync between the proxy instances does not work.

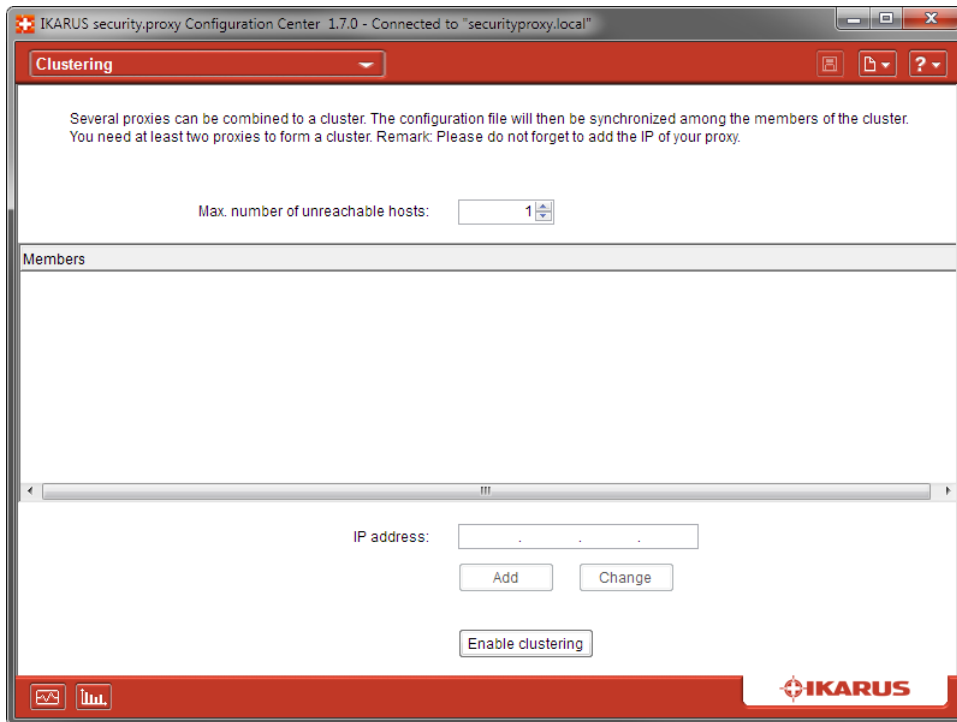


Figure 36: Clustering

Item	Description
Max. number of unreachable hosts	The maximum number of hosts in the cluster that may be not reachable or have failed. When this number has been reached, soft stopping the remaining <b>IKARUS security.proxy</b> instances is not possible any more.
Members	List of <b>IKARUS security.proxy</b> instances contained in this cluster.
IP address	IP address of the <b>IKARUS security.proxy</b> instance to be added to the cluster.
Button "Add"	Clicking this button adds the entered IP address to the list of proxy servers.
Button "Change"	Allows for changing an IP address that has already been entered.
Button "Enable clustering" / "Disable clustering"	Clicking this button enables or disables clustering. Note that all changes become effective only after saving them.

Table 31: Clustering

### 3.13 WCCP

In an network with multiple instances of **IKARUS security.proxy** running, WCCP can be used to configure IP package forwarding.

One instance has to be configured as being the Designated Web Cache. This one is responsible for distributing the incoming traffic to all the other **IKARUS security.proxy** instances.

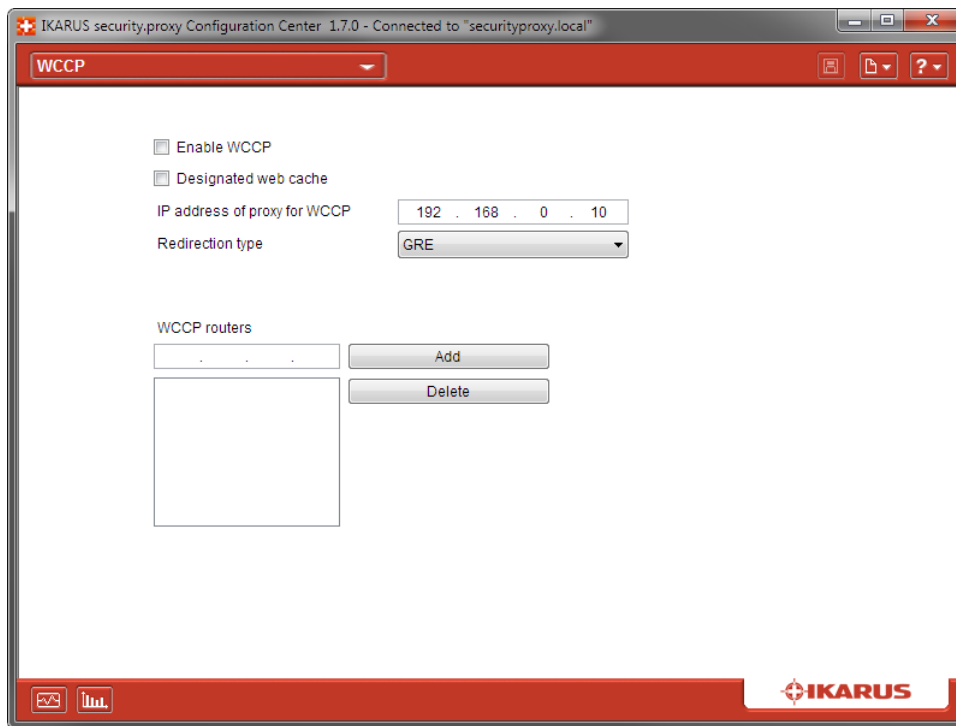


Figure 37: WCCP

Wert	Beschreibung
Enable WCCP	Enable/disable WCCP.
Designated Web-Cache	Makes this instance of <b>IKARUS security.proxy</b> the master. This one is responsible for distributing packages to all other instances.
IP address of proxy for WCCP	IP address of this instance. Has to be set to ensure matching of the connections IP address and the public IP address.
Redirection type	<b>GRE:</b> Forward packages to proxies using GRE <b>Layer2:</b> Forward by rewriting the destination MAC address
WCCP routers	List of WCCP routers to be connected

Table 32: WCCP

## 3.14 Reporting

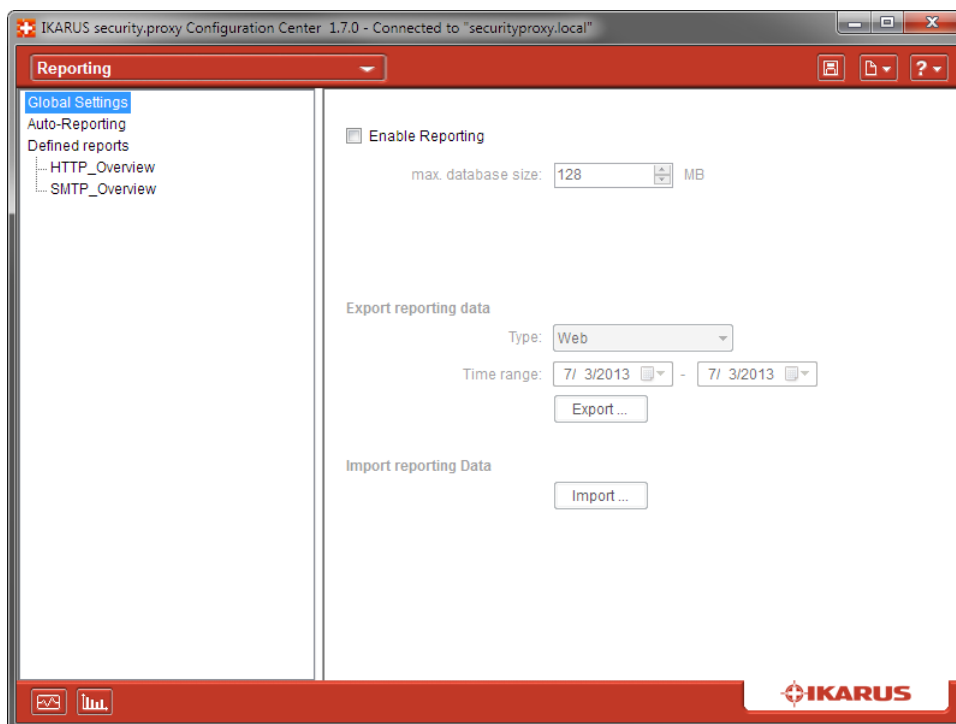
**IKARUS security.proxy** allows for creating graphical reports that provide information on your Internet activity and the amount of your e-mail based on specific criteria.

Reports are configured in the Reporting dialog and can be displayed in the report-view window. In addition, that dialog allows for configuring database settings.

The dialog provides four functionalities:

- Configuring global reporting settings
- Create and send reports automatically
- Creating reports using templates
- Editing existing reports

### 3.14.1 Global Settings



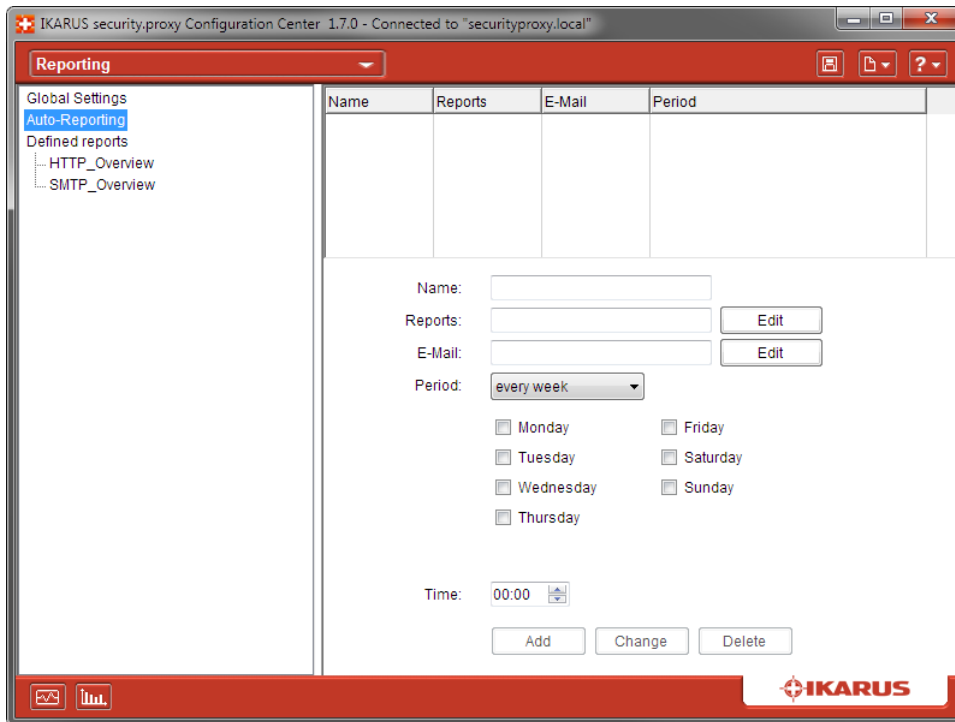
**Figure 38:** Reporting: Global Settings

Item	Description
Enable Reporting	Enables <b>IKARUS security.proxy</b> reporting. If reporting is not enabled, no information will be logged. Re-enabling the reporting function will restart logging; this means that no data for the period of time where reporting was disabled will exist on the database.
Max. Database Size	Sets the database size (in MB) on your disk. Whenever this amount is exceeded, the oldest 5 percent of data will be deleted.*
Database Path	Sets the database location.
Exporting Report Data	
Type	Determines the type of data to be exported.
Time Range	Sets the period of time for which data will be exported.
Button "Export"	Click this button to launch a Save dialog where you can save the exported data in CSV format.
Import Reporting Data	
Button "Import"	Click this button to import a CSV file to the database. The CSV file must have the export structure.

**Table 33:** Reporting: Global Settings

\* When deleting the oldest 5 per cent of data from the database, the program refers to the insertion date rather than the actual date of the respective item. Therefore, imported data might be the last to be deleted. This auto-delete approach might result in gaps when imported CSV files contain old records.

### 3.14.2 Auto-Reporting



**Figure 39:** Reporting: Auto-Reporting

Item	Description
Name	The name for the Auto-Reporting entry.
Reports	A list of reports, that are to be created and sent automatically. The reports can be chosen in a separate dialog window, which can be accessed by clicking on the "Edit" button.
E-Mail	Recipients for the automatically created reports. The button "Edit" opens a dialog window, where the user can enter e-mail addresses.
Period	This drop-down list selects whether reports shall be created and sent on days of a month or days of a week.
Weekdays/Days of Month	Depending on the period setting, days of a week (Monday-Sunday) or days of a month (1-31) can be selected. Attention: No report will be sent on days 29 to 31 if the current month has fewer days than that.
Time	Time of the day for the reports to be created and sent.
Button "Add"	Adds a new entry with the given input data.
Button "Change"	Overwrites the selected entry with the given input data.
Button "Delete"	Deletes the selected Auto-Reporting entry.

**Table 34:** Reporting: Auto-Reporting



### 3.14.3 Creating a New Report

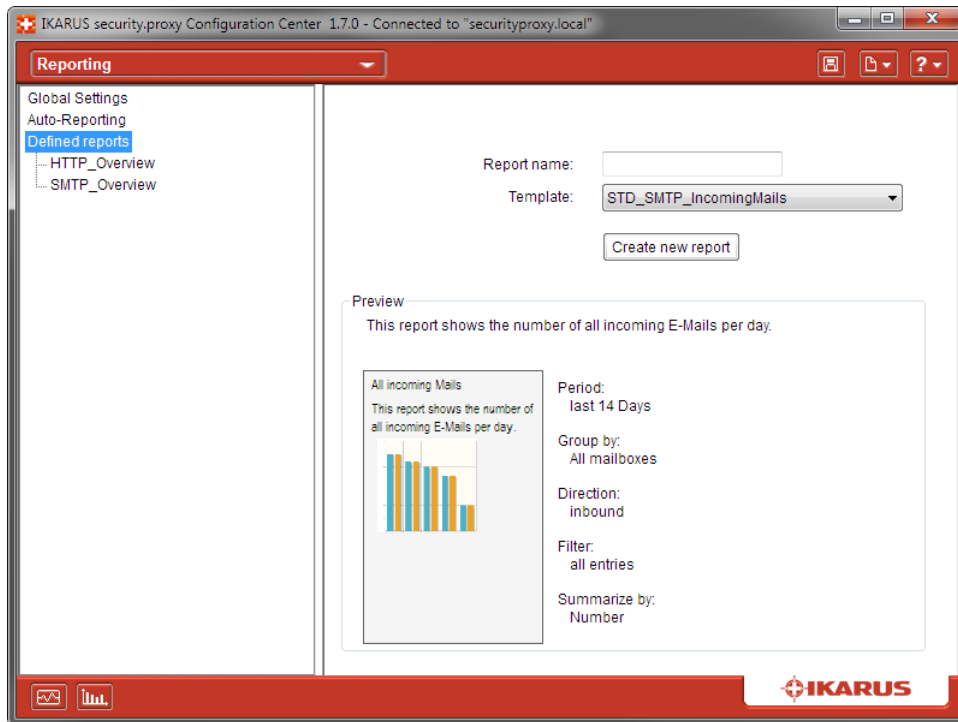


Figure 40: Reporting: Create a new report

Item	Description
Report Name	Sets the name of the report to be created.
Template	Allows for choosing the desired template from a list. The new report will be based on the template defaults, which can still be changed afterwards.
Button "Create New Report"	Clicking this button will create the new report and add it to the list and the report-view dialog.
Preview	This area provides a graphical preview of the report type and the filter defaults of the selected template.

Table 35: Reporting: Create new report

### 3.14.4 Defined Reports

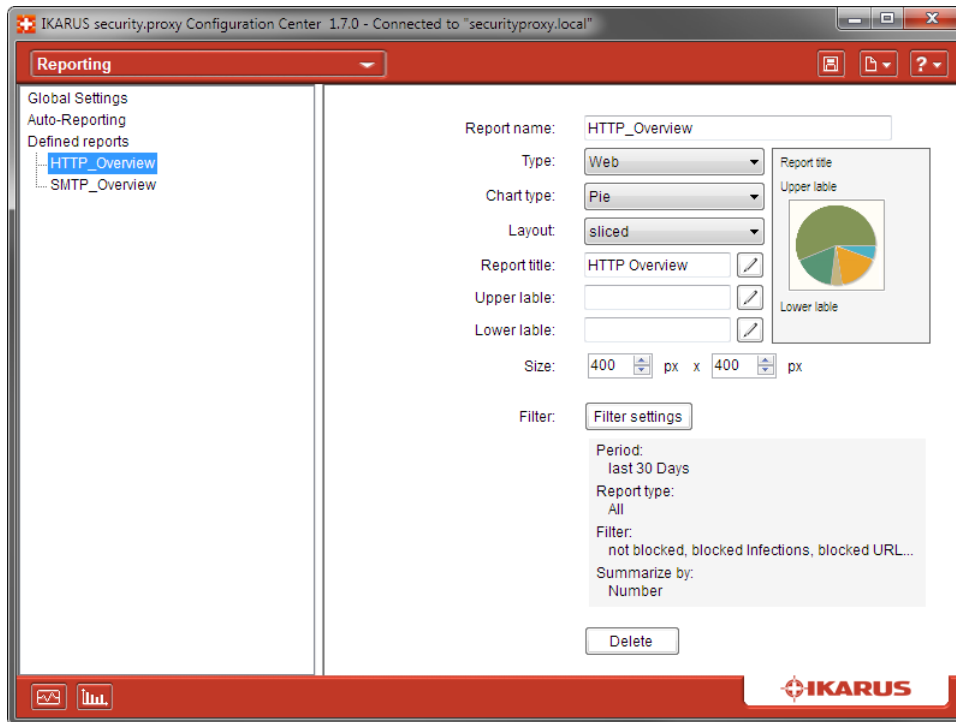


Figure 41: Reporting: Defined reports

Item	Description
Report Name	The report name (or the name of the report file)
Type	Sets the report type (Web or Mail).
Chart Type	Sets the chart type (bar, pie or line chart or as table).
Layout	Sets the layout type of the chart. This depends on the selected chart type (e.g. vertical bars).
Report Title	This is the report header.
Upper Label	Explanatory text to be displayed right above the report
Lower Label	Explanatory text to be displayed below the report
Edit	Clicking this button will open a dialog for text editing.
Size	Report size (width x height, in pixels)
Button "Filter Settings"	Clicking this button will open a dialog for editing the filter settings of the selected report type. The list below the button shows the current filter settings.
Button "Delete"	Clicking this button will delete the selected report.

Table 36: Reporting: Defined reports

Newly generated and edited reports will be displayed in the report-view dialog only after saving. This is because data collection and evaluation are proxy-based.

### Chart Types and Layout Types



Figure 42: Reporting: Chart types and layout types

### Filter Settings for the Web Type

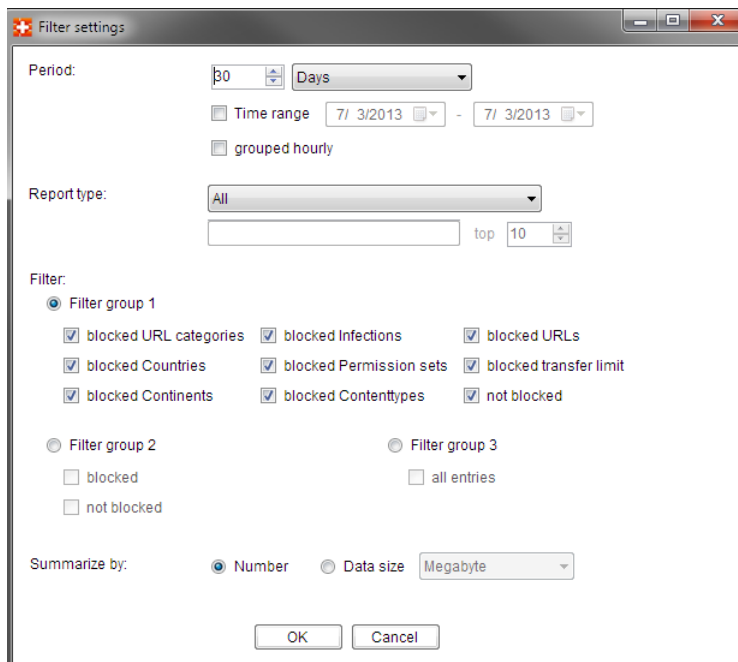
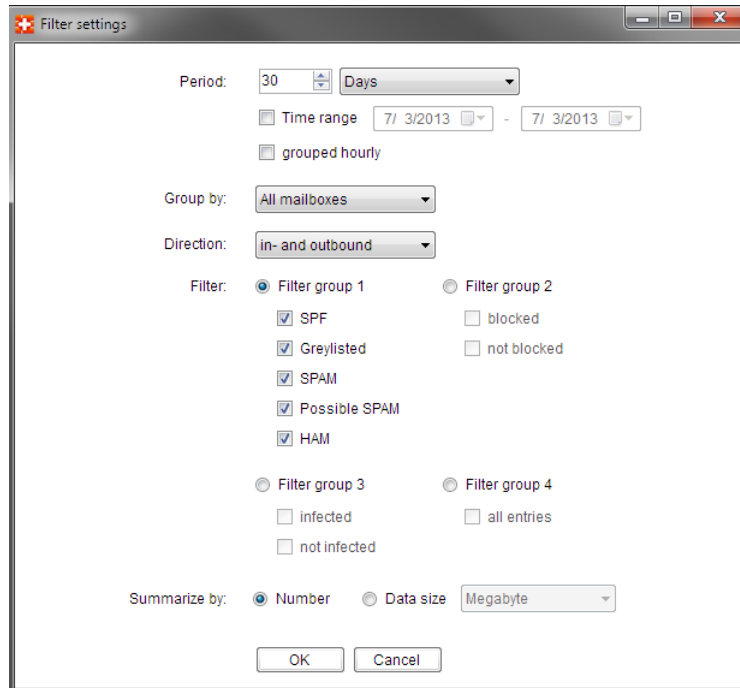


Figure 43: Reporting: Filter settings (Web)

Item	Description
Period	Specifies the evaluation period. You can either enter a number and select a unit (hours, days, weeks, months, quarters or years) or specify a date range. The maximum number that can be entered is 100. "Week" refers to a calendar week. Units start at the respective first unit (for example, the first day of the month, or midnight as the first hour of a day).
Hourly Grouped	All items will be grouped by the hour, resulting in a report where all items will be grouped and summed up by the time they occurred (00:00-01:00, 01:00-02:00, etc.).
Group By	There are different grouping options: <ul style="list-style-type: none"> <li>• Select all records.</li> <li>• Group by permission set, source IP address, domain, top-level domain (TLD), network group or subnet using the respective parameter.</li> <li>• Group by subnets in network groups, permission set, source IP address, domain, or TLD based on the largest number of or the largest data amount for requests. The top items will be selected.</li> <li>• Group by a specific permission set, source IP address, network group or subnet (including parameter). This option shows the domains or TLDs that are most frequently listed or produce the largest amount of data.</li> <li>• Group by customers per site (network group or subnet), where a customer is defined as a unique source IP address per hour.</li> </ul>
Filter	Filter groups allow for narrowing selected data for analysis. The total of all flags within a filter group is always 100 %.
Filter Group 1	Allows for selecting and filtering by reasons for blocking.
Filter Group 2	Provides a summary of all reasons for blocking.
Filter Group 3	No filtering will be performed. All items will be evaluated.
Summarize By	Select whether the summary will include the total number of items or the total data volume (including the unit—KB, MB, or GB).

**Table 37:** Reporting: Filter settings (Web)

### Filter Settings for the Mail Type



**Figure 44:** Reporting: Filter settings (Mail)

Item	Description
Period, Hourly Grouped, Summarize By	Same as with the filter settings for the Web Type
Group By	There are three options: <ul style="list-style-type: none"> <li>• Select all records.</li> <li>• Group by mailbox (including parameter).</li> <li>• Group by mailbox based on the largest number of messages or the largest messages. The top items will be selected.</li> </ul>
Direction	Specifies whether incoming and/or outgoing mail will be evaluated.
Filter	Filter groups allow for narrowing selected data for analysis. The total of all flags within a filter group is always 100 %.
Filter Group 1	Filters by message rating (i.e. blocking due to SPF or greylisting, or by SPAM rating).
Filter Group 2	This group allows for distinguishing between blocked and non-blocked messages. Note the SPAM mail might be included in the Blocked category if the SPAM settings configure deletion or redirection of messages.
Filter Group 3	This allows for filtering by infected or non-infected messages.
Filter Group 4	No filtering will be performed. All items will be evaluated.

**Table 38:** Reporting: Filter settings (Mail)

### 3.15 Log Files

Select the Log Files item to access the **IKARUS security.proxy** log files. The following items are available:

- **Global:** Content of the file `splogfile.log`
- **Web:** Content of the file `proxy.log`
- **E-Mail:** Content of the file `mail.log`
- **Update:** Content of the file `update.log`

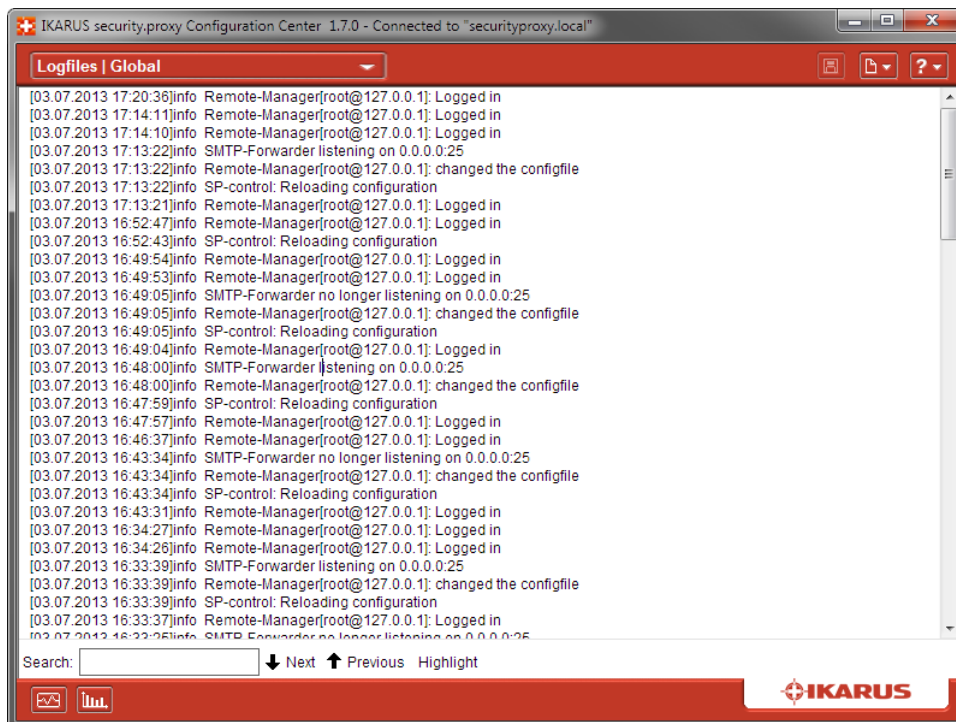


Figure 45: Log files

### 3.16 Config File

Select this item to view and edit the `securityproxy.conf` file. You can manually retrieve and edit all configuration parameters that can be set in the **IKARUS security.proxy Configuration Center**.

Only make changes to the configuration file if this is crucial; editing the `securityproxy.conf` file manually should normally be avoided. You should rather use the **IKARUS security.proxy Configuration Center** for that purpose because it allows for managing all options safely and conveniently.

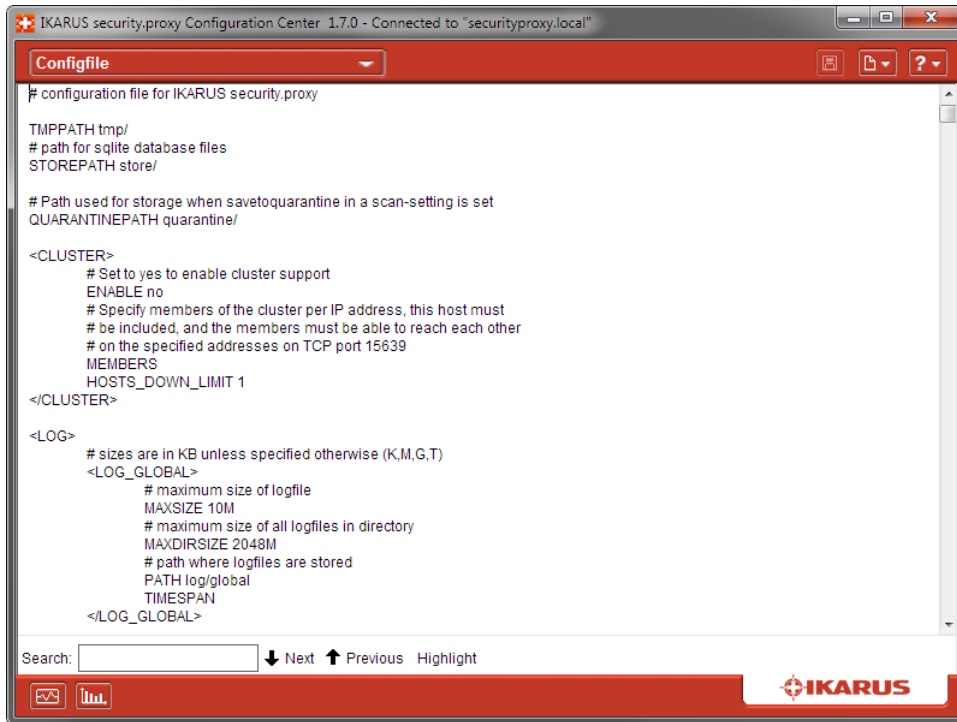


Figure 46: Configuration file

### 3.17 Virus List

IKARUS security.proxy monitors all incoming data (HTTP, SMTP, POP3, etc.) and includes all malware it has found into this list. Double-click any entry to view relevant details.

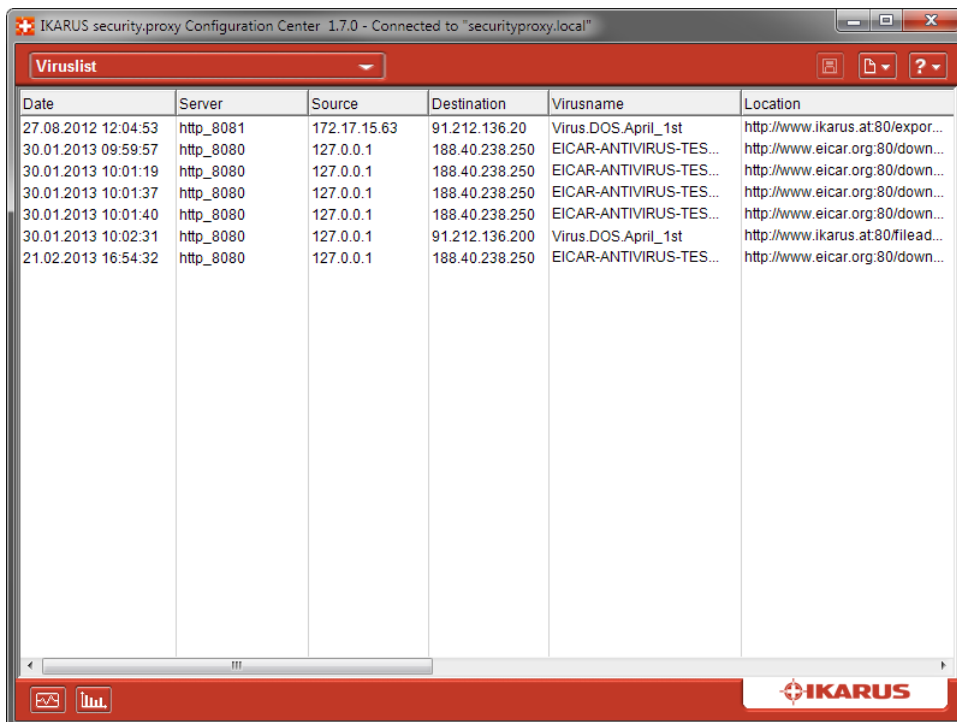


Figure 47: Virus List

### 3.18 Activity Monitor

The **IKARUS security.proxy** allows you to overview the activities of its users. You can monitor the mailing and surfing behaviors of the users.



With the button shown in the bottom line of the **IKARUS security.proxy Configuration Center** you can activate the ActivityMonitor.

This dialog can be shown while using the **IKARUS security.proxy Configuration Center**, but it will get closed if the **IKARUS security.proxy Configuration Center** does.

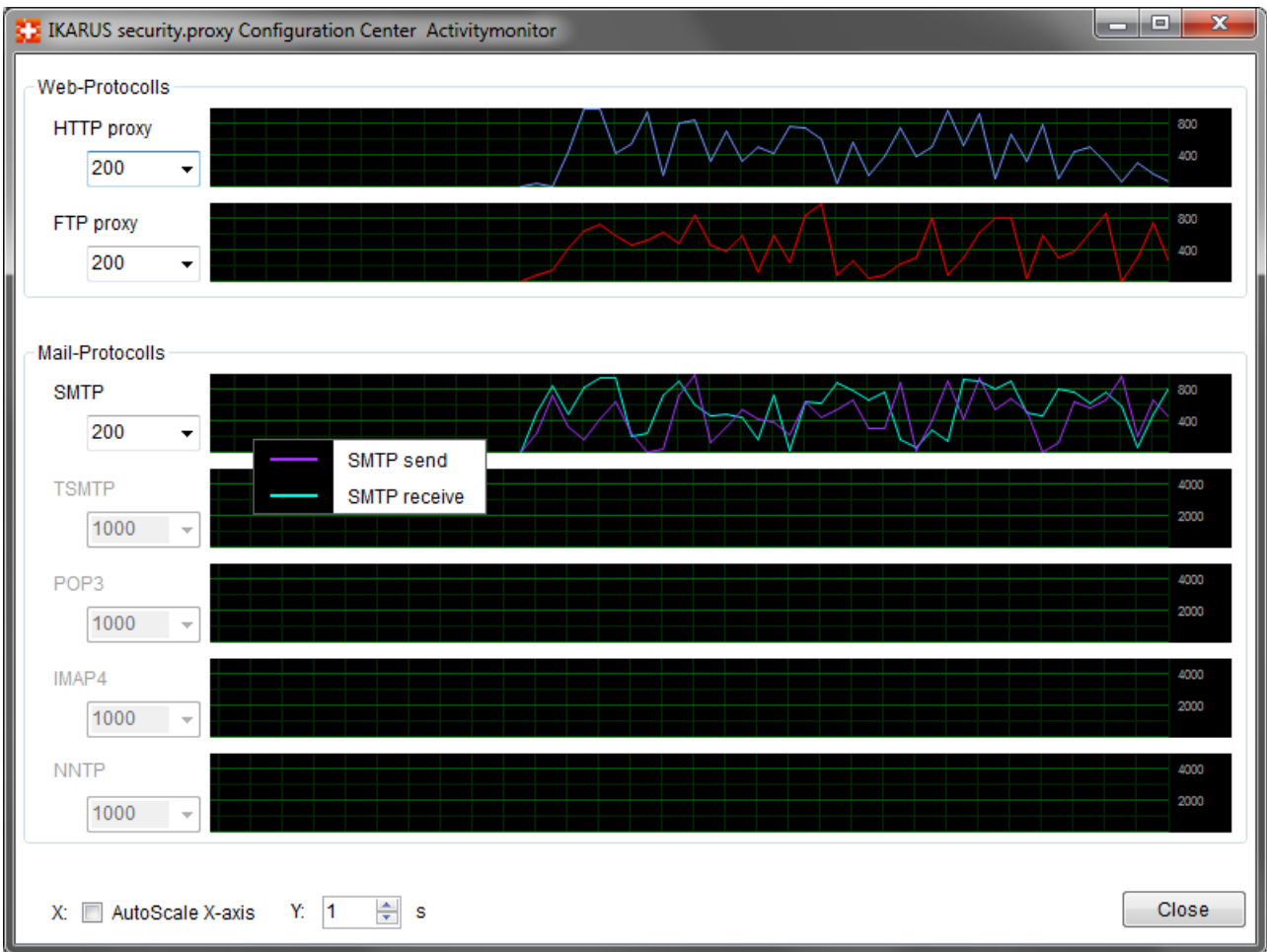


Figure 48: ActivityMonitor

Only activated protocols can be monitored, inactive protocols will be disabled.


For a better usage this monitors can each be scaled on X axis and y axis or simply use the auto scale functionality.



### 3.19 Show Reports

This dialog allows you to show the reports you configured and saved in the configuration file.

You can open this dialog in two ways:

1. Use the shown button in the bottom line of the **IKARUS security.proxy Configuration Center**: 
2. Use the Reporting-button in the Login dialog. You need a valid user and password to use this.

Both methods will open the following dialog in which the reports can be shown:

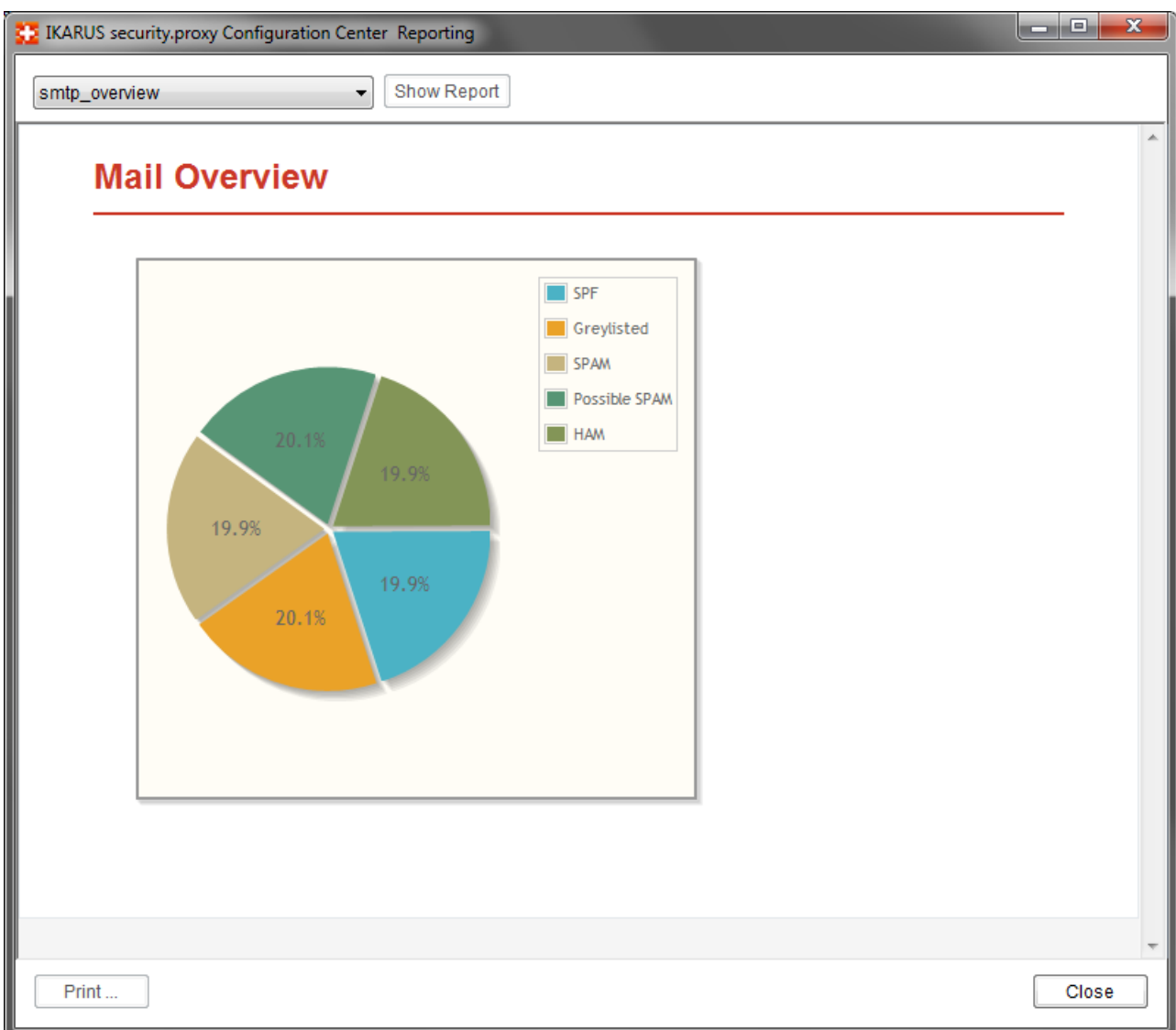


Figure 49: Show Report

Item	Description
Button "Show Report"	The report chosen in the drop down list will be shown in the empty field below.
Button "Print ..."	Opens the Print dialog.
Button "Close"	Closes the dialog.

**Table 39:** Show Reports

## 4 Using the IKARUS security.proxy

### 4.1 Using IKARUS security.proxy as an MX Gateway

#### 4.1.1 Overview

**IKARUS security.proxy** can be used as Mail Exchange (MX) Gateway, thus allowing for receiving incoming e-mail with no viruses or spam. This type of application requires you to run your own DNS server in your domain for making the necessary MX entry. In addition, we assume that a dedicated mail server exists in your internal corporate network.

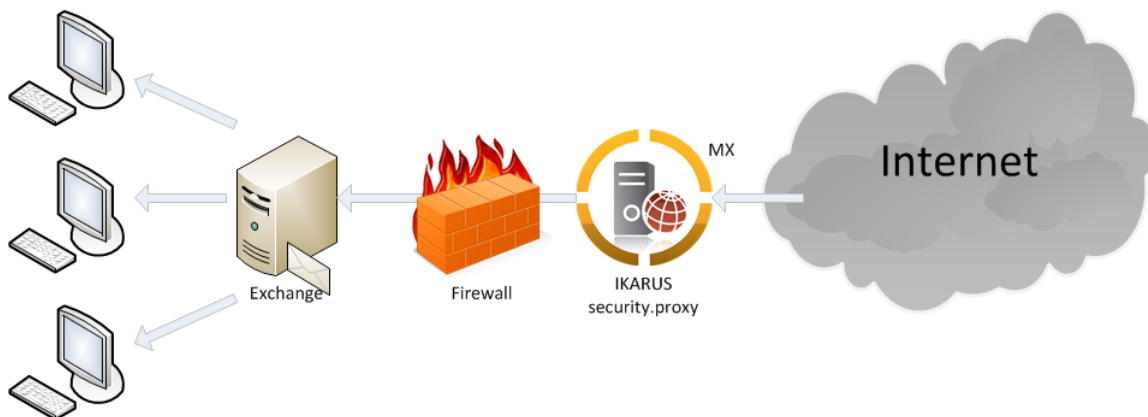


Figure 50: Overview MX Gateway

#### 4.1.2 Prerequisites

The MX entry of your domain must be configured to point to the externally accessible IP address of **IKARUS security.proxy**. When setting up your firewall, ensure that **IKARUS security.proxy** can be accessed from the Internet.

#### 4.1.3 Settings in IKARUS security.proxy

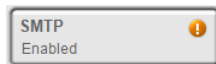
In this section, we assume that the SMTP service in **IKARUS security.proxy** has been disabled.


1. For using **IKARUS security.proxy** as an MX Gateway, the IP address used for access from the Internet needs to be bound. For this purpose, you need to provide either the IP address of the network adapter or 0.0.0.0 if you want **IKARUS security.proxy** to listen to all network interfaces available (this is the default setting). Be sure to use the SMTP default port 25 for MX-gateway operation.
2. Next, you need to define routes for incoming e-mail. In doing so, you configure how to handle incoming mail. For instance, if your internal mail server is named `exchange.example.com` and the domain to be monitored is `@example.com`, provide the following settings:
  - (a) Type: Target Domain / E-Mail. Enter the target domain (`example.com`) into the text box.
  - (b) Select the scan rule to be applied.
  - (c) Direction: Inbound.

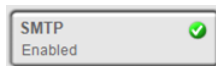
- (d) Select whether to apply greylisting or SPF1.
  - (e) Action: Select the host and provide the computer names or the target-server IP address. The target server must be a SMTP server bound to port 25.
3. Click the Add button to add the newly created route setting to the Routes list. If necessary, you can now change the priorities of the supplied routes.
  4. Select the SMTP node from the overview tree. A red indicator shows that the SMTP service is currently disabled.



5. Click the SMTP button. The indicator will turn yellow to show the upcoming status change of the service.



6. Next, click the  button. This will enable the SMTP service with the selected settings. If SMTP is successfully enabled, the indicator will turn green.



## 4.2 Using IKARUS security.proxy as a Mail Relay

### 4.2.1 Overview

IKARUS security.proxy can also act as a relay server for outgoing e-mail. This ensures that outgoing e-mail, too, is checked for spam and malware.

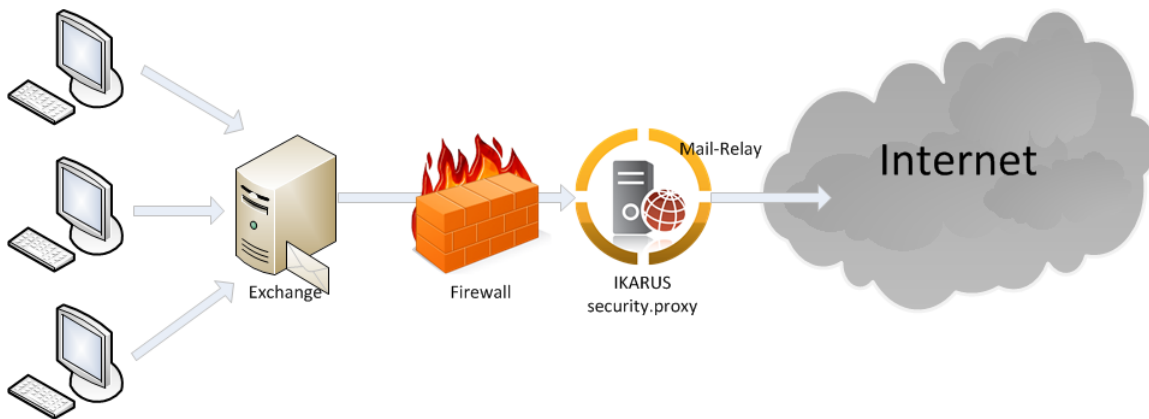


Figure 51: Overview Mail Relay

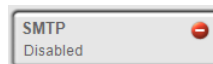
### 4.2.2 Prerequisites

The internal firewall of your organization must be configured to allow all computers that send e-mail to access **IKARUS security.proxy**. In addition, changes to the configuration of your internal mail server may be required to enable relaying of outgoing e-mail over **IKARUS security.proxy**. Refer to the documentation of your mail server.

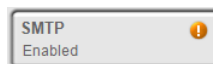
### 4.2.3 Settings in IKARUS security.proxy


In this section, we assume that the SMTP service in **IKARUS security.proxy** has been disabled.

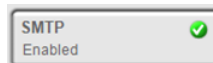
1. For using **IKARUS security.proxy** for relaying e-mail, the IP address used for accessing the service needs to be bound. For this purpose, you need to provide either the IP address of the network adapter or 0.0.0.0 if you want **IKARUS security.proxy** to listen to all network interfaces available (this is the default setting). Note: For security reasons, be sure not to bind 0.0.0.0 when using **IKARUS security.proxy** as an outgoing relay only.
2. Next, you need to define routes for outgoing e-mail. In doing so, you configure how to handle outgoing mail. For example, if your internal mail server has the IP address 10.0.0.10 and you want to relay e-mail from that server only, make the following settings in the Settings / Routes form:
  - (a) Type: Client IP Mask. Enter the IP address of the internal mail server (10.0.0.10/32) into the text box.
  - (b) Select the scan rule to be applied.
  - (c) Direction: Outbound
  - (d) Action: Mail routed to the Internet requires the MX action to be selected. This way, **IKARUS security.proxy** can forward the e-mail messages to the appropriate target server.
3. Click the Add button to add the newly created route setting to the Routes list. If necessary, you can now change the priorities of the supplied routes.
4. Select the SMTP node from the overview tree. A red indicator shows that the SMTP service is currently disabled.



5. Click the SMTP button. The indicator will turn yellow to show the upcoming status change of the service.



6. Next, click the  button. This will enable the SMTP service with the selected settings. If SMTP is successfully enabled, the indicator will turn green.



If there are multiple computers that you want to use for transmitting e-mail over **IKARUS security.proxy** on the internal network, you can either add them separately or, if they all belong to the same subnet, provide the network address and the subnet mask (e.g. 192.168.0.0/24).

## 4.3 The URL Filter

**IKARUS security.proxy** 's URL filter allows for "administering" the Internet by subjects or sites.

### 4.3.1 How to Configure the URL Filter?

The URL filter currently handles three main areas:

- URL categories
- Country filters
- Continent filters

Setting up the filter is the same for all of the three categories:

- Open a permission set.
- Make a selection in the type drop-down menu.

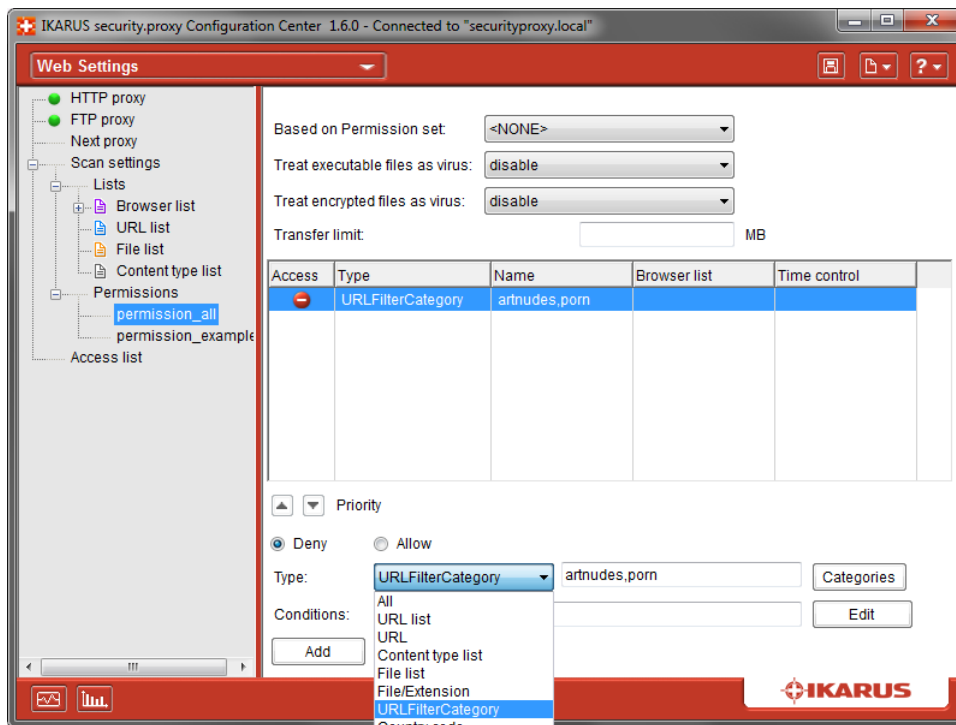
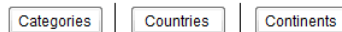


Figure 52: URL filter

- Click the appropriate button on the right.



- Check the desired categories, countries, or continents in the list, then click OK. Below is a sample of URL filter categories:

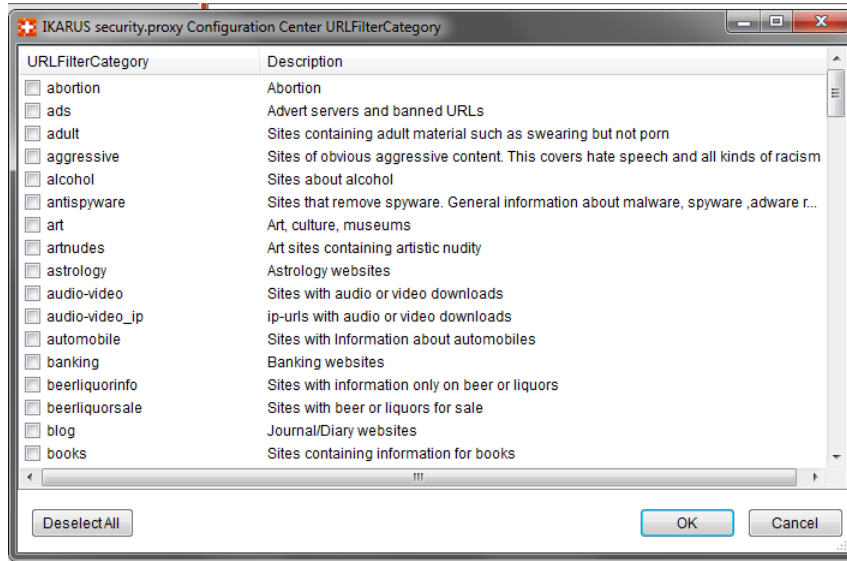


Figure 53: URL filter categories

- Next, add the desired permission.

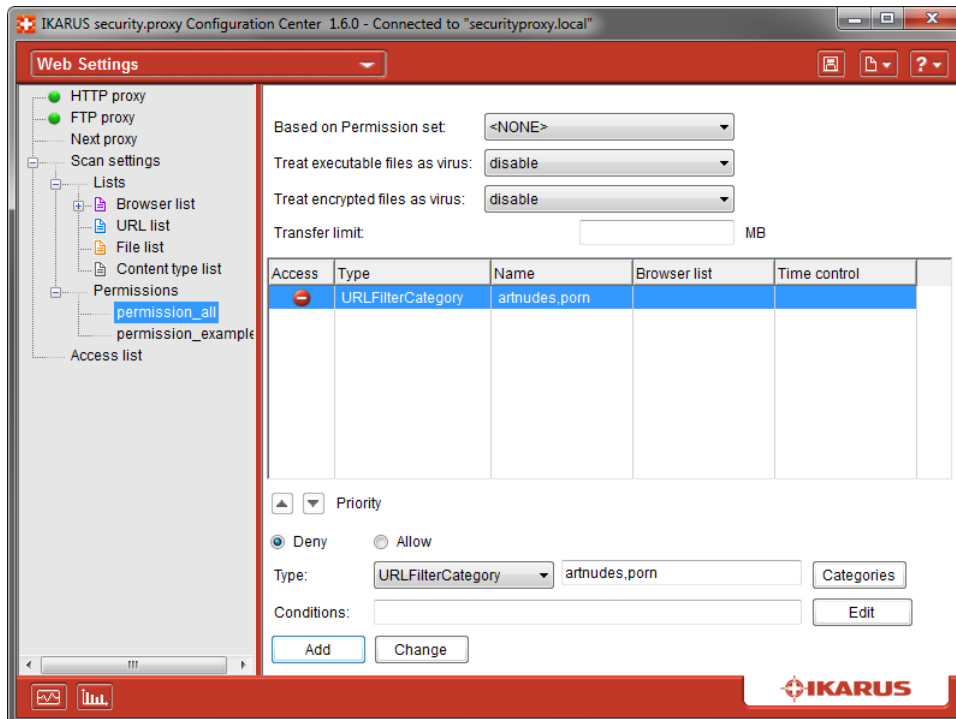


Figure 54: Permissions

Example:

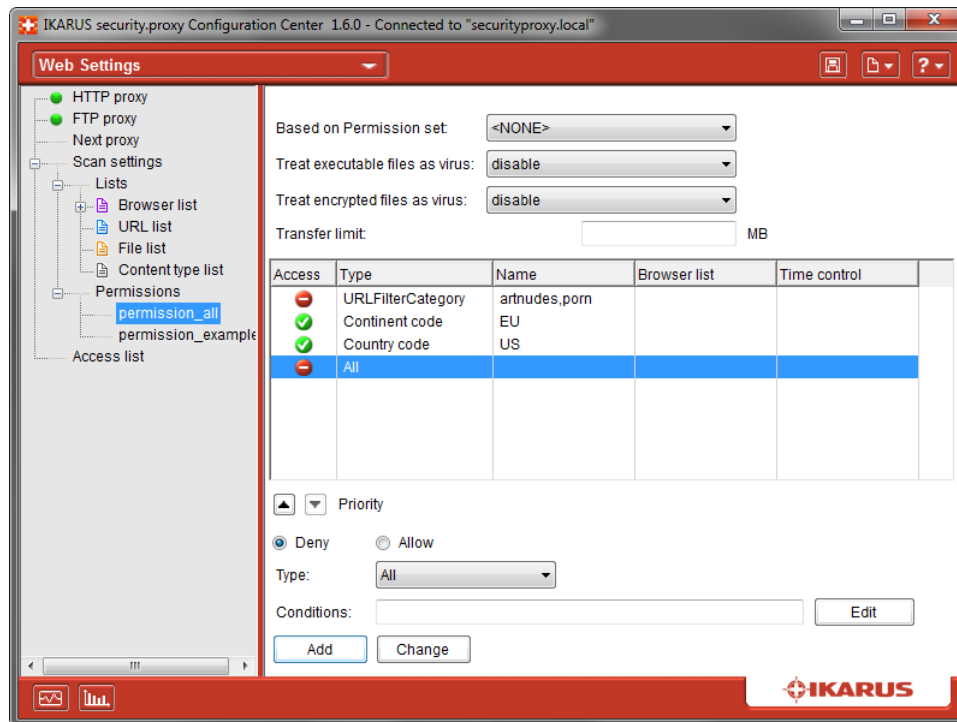


Figure 55: Permission sets

The above permission set has the following effects:

- All URLs from the "artnudes" and "porn" categories are blocked.
- All URLs from the European Union (except for those from the above categories) are allowed.
- The same is true for all URLs from the United States of America.
- All other traffic will be blocked.

As a result, all URLs except from those from US and the EU that are not from the "artnude" and "porn" categories will be blocked.

### 4.3.2 Branding

**IKARUS security.proxy** shows different web sites whether the user signs in for web access or wenn er sich für den Internetzugang anmeldet, oder der Zugriff auf eine bestimmte Seite geblockt wird.

These web pages can be designed individually for different network providers. Such a set of individual designs will be referred to as "branding".

The HTML templates for the different brandings are placed in subfolders of `conf` named according to the branding.

```
conf/
  messages/
    filiale1/
```



```
lockpage.html
filiale2/
lockpage.html
```

```
...
```

Access to the resources referenced in these templates (CSS, Images, etc.) must be ensured by the web server's configuration.

By setting the branding for entries in the access list (see 3.9.5) they apply for the selected IP address, or subnet, respectively.

## 4.4 Sending E-Mail over TLS

### 4.4.1 Overview

**IKARUS security.proxy** is capable of sending and receiving encrypted e-mail using the Transport Layer Security (TLS) protocol.

### 4.4.2 Prerequisites

You do not need to make any configuration settings for enabling TLS but just a key file and a certificate file. You may create the two files yourself, for example, using OpenSSL. The certificate file requires a signature either from yourself or from a certificate authority (CA).

You may refer to one of the myriads of tutorials on the Web for information on how to create self-signed certificates. However, for security reasons, certificates for use in production environments should be issued by a recognized CA.

Be sure to store the key and certificate files in the following subdirectory of the **IKARUS security.proxy** installation folder:

```
/IKARUS/security.proxy/conf/certs
```

While you can assign any name to the files, be sure to use the CRT and the KEY file extensions for the certificate file and the key file, respectively.

After storing the files and restarting the SMTP service, **IKARUS security.proxy** is ready for sending and receiving e-mail over TLS.

- E-mail will automatically be transmitted over TLS if the target server supports TLS. In any other case, unencrypted e-mail will be sent.
- E-mail reception over TLS depends on whether the sending server supports TLS and initiates e-mail transmission over TLS.

### 4.4.3 How to Verify if TLS is enabled

To verify if the key and certificate files have been applied properly, establish a Telnet connection to **IKARUS security.proxy**:

```
Client (C): telnet <servername> 25
Server (S): 220 <servername> \isp SMTP-Server ready
C: EHLO foo
S: 250-<servername>
    250 STARTTLS
C: QUIT
S: 221 closing connection
```

Verify that **IKARUS security.proxy** responds to the EHLO command with "250 STARTTLS". This indicates that the server is ready to accept TLS connections. If OpenSSL is installed on your system, you may also check for the TLS handshake using the following command on the command line:

```
% openssl s_client -starttls smtp -crlf -connect <servername or IP-Address>:25
```

## 4.5 How to Configure for LDAP Authentication

### 4.5.1 Overview

This tutorial describes how to configure **IKARUS security.proxy** in conjunction with an LDAP server (e.g. Windows Active Directory). The setup allows for authenticating domain users when using the HTTP proxy.

The Lightweight Directory Access Protocol (LDAP) allows for querying and editing a directory service over an IP network. Active Directory from Microsoft is probably the best-known directory service. It is part of Microsoft server products including Windows 2008, Windows Small Business Server, etc.

LDAP provides for authenticating Active Directory users and groups using **IKARUS security.proxy**. This way, you can configure, for example, specific permission sets based on the groups a user belongs to. Users log in to **IKARUS security.proxy** using their domain-user ID and password and will then be granted appropriate web-browsing rights based on their group memberships.

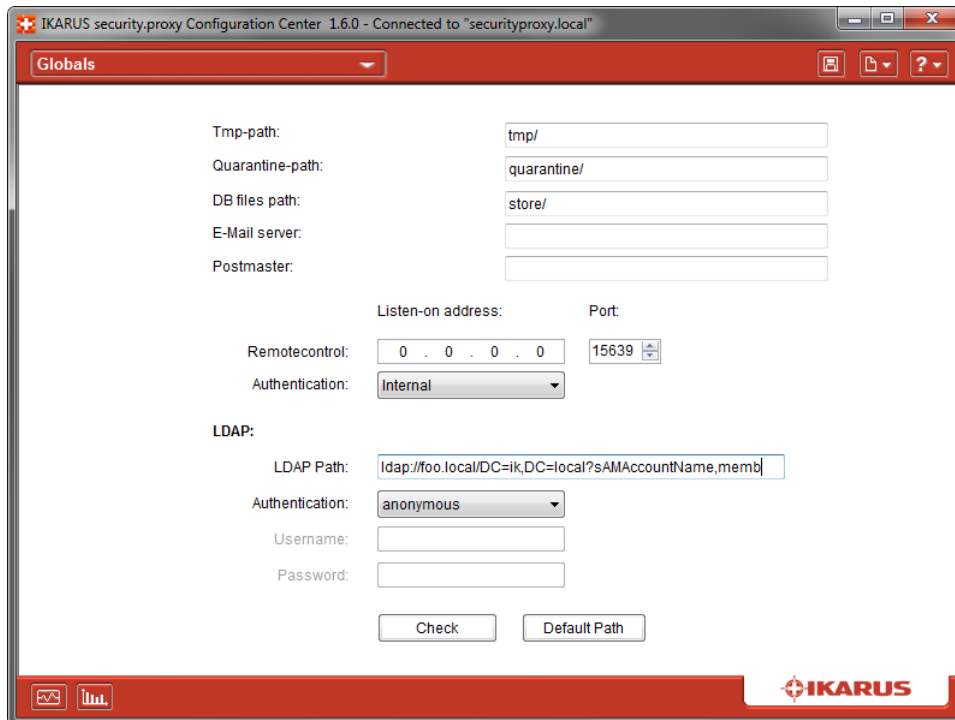
### 4.5.2 Prerequisites

The following prerequisites must be met for using **IKARUS security.proxy** with LDAP:

- A configured LDAP server (for example, a Windows domain controller) must be available and accessible to **IKARUS security.proxy**.
- You need to specify a domain user for querying LDAP information. (Essentially, any domain-user account can be used for that purpose; however, for security reasons, we recommend creating a dedicated user.)

### 4.5.3 LDAP Path Settings

For establishing the connection between **IKARUS security.proxy** and the LDAP server, you need to provide the LDAP path. The setting is found in the Global menu.



**Figure 56:** Definition of LDAP path

The LDAP path has the following structure:

```
ldap://foo.local/DC=ik,DC=local?sAMAccountName,memberOf?sub?(objectClass=person)
```

Note: Be sure to replace foo.local with the actual domain name.

Tip: We recommend using LDAPS for secure LDAP-data transmission. For this purpose, change ldap:// at the beginning of the LDAP string to ldaps://. However, you first need to make sure that you are LDAP server supports LDAPS.

If you configure **IKARUS security.proxy** using the **IKARUS security.proxy Configuration Center** and the server where **IKARUS security.proxy** is installed is a member of a domain, just click the "Default Path" button to provide the correct LDAP path.

**IKARUS security.proxy** offers two ways of authenticating with the LDAP server:

- Anonymous authentication (if the LDAP server supports this)
- Simple authentication (you require a valid domain-user ID and password)

Click the 'Check' button to verify the accuracy of your entry before saving it.

#### 4.5.4 Creating Permission Sets for LDAP Groups

Next, you create permission sets for LDAP groups in the Web Settings. This section describes how to do this in a Microsoft Windows 2008 sample environment.

Let us assume that you have three organizational units: Finance, Sales, and Management. You have created a group with the respective name for each of the three units. The next step is to create a specific permission set for each of the groups. Each permission set will reflect the browsing permissions of the associated group.

First, create a permission set for each of the groups. The group names must exactly match the respective Active Directory group names; however, they must be prefixed to ensure that **IKARUS security.proxy** correctly matches them correctly. We recommend using a meaningful prefix such as group\_.

Now, create the group\_finance, group\_sales, and group\_management permission sets, and configure appropriate permissions (e.g. URL filters, virus protection, etc.) for each group.

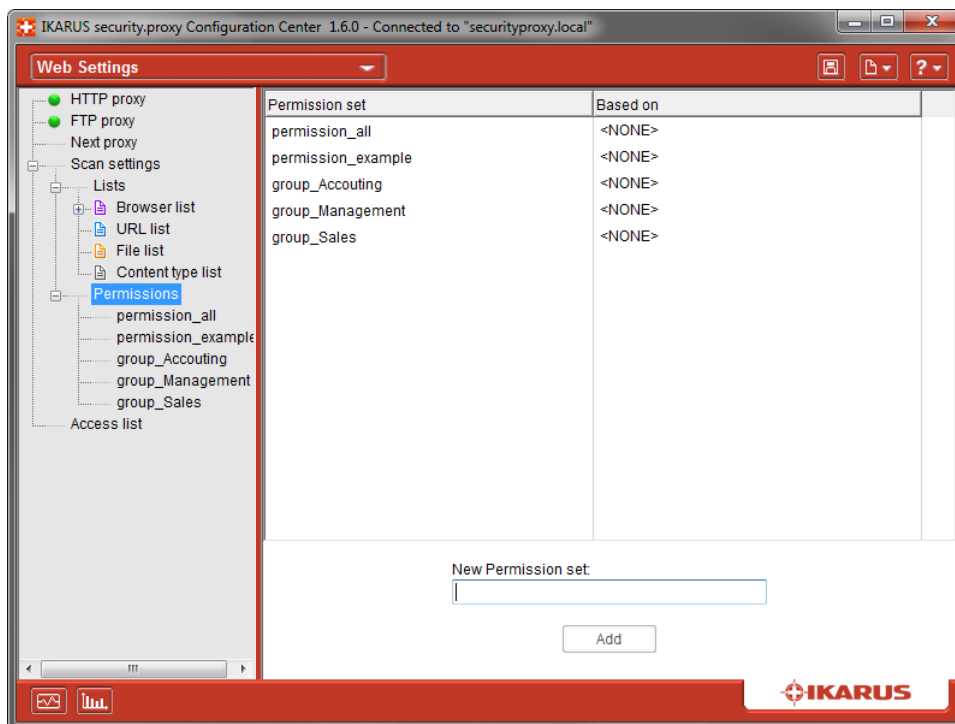


Figure 57: Creating permission sets for LDAP groups

Save your changes.

#### 4.5.5 Creating Access Lists for LDAP Authentication

Finally, you need to create access lists for using LDAP. For each access list, define network settings and access permissions as appropriate and select the LDAP Authentication option from the Authentication drop-down menu. Enter group\_%g into the Permissions Set per Mask field. Complete the operation by clicking the 'Add' button.

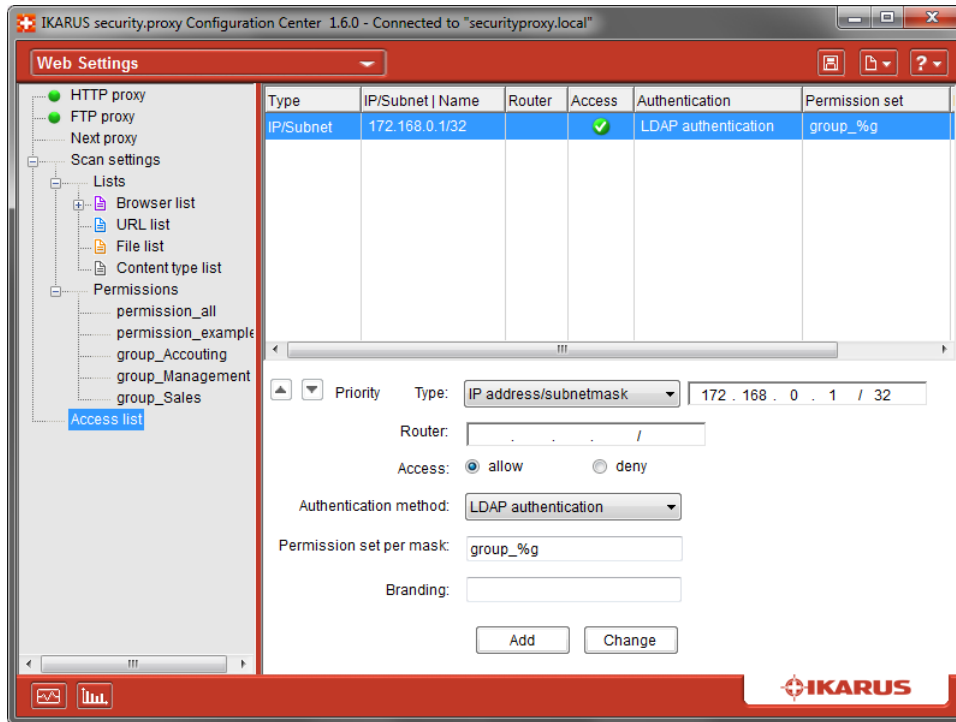


Figure 58: LDAP access list

Save your changes.

**IKARUS security.proxy** is now ready for using LDAP.

#### 4.5.6 Using LDAP Authentication in Your Browser

If the browser of your choice has been configured for use with **IKARUS security.proxy**, the user will be prompted for entering an ID and a password whenever he or she tries to access a web page for the first time after launching the browser. Here, the user needs to enter the same ID and password used for logging in at the Windows domain.

## 4.6 Safe Web Browsing with IKARUS security.proxy

**IKARUS security.proxy** can be used as a HTTP filter and therefore allows for browsing the Web safely. Please note that **IKARUS security.proxy** allows unlimited HTTP access when using the default configuration.

### 4.6.1 How to Browse the Web using IKARUS security.proxy

To use **IKARUS security.proxy** with the default configuration, enable the HTTP service if necessary (enabled by default) and enter the proxy server into your browser.

To enable the HTTP service in **IKARUS security.proxy**, click the button, and then store your changes.

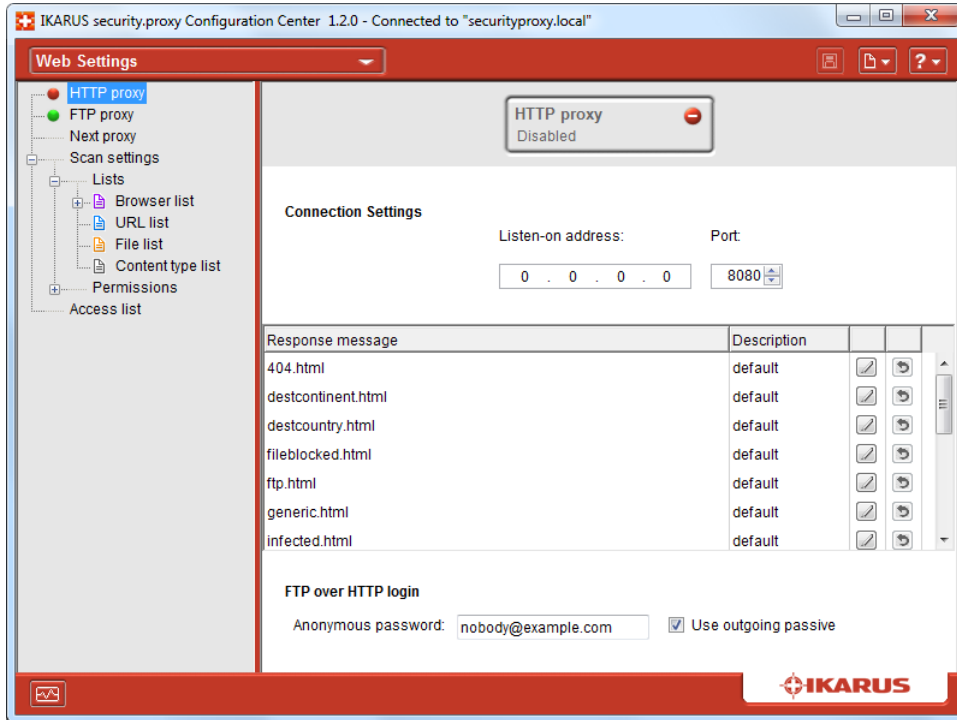


Figure 59: HTTP proxy settings



If you prefer not to use the default configuration, follow the steps below to create a permission set and add it to the access list.

Creating a permission set:

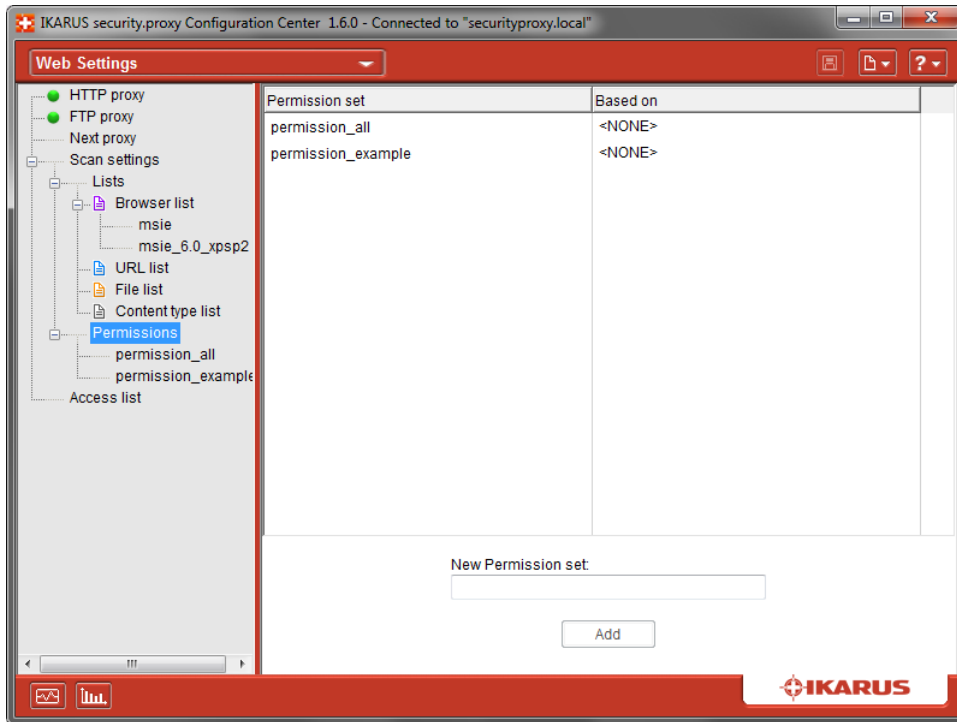


Figure 60: Creating permission sets

Adding the permission set to the access list:

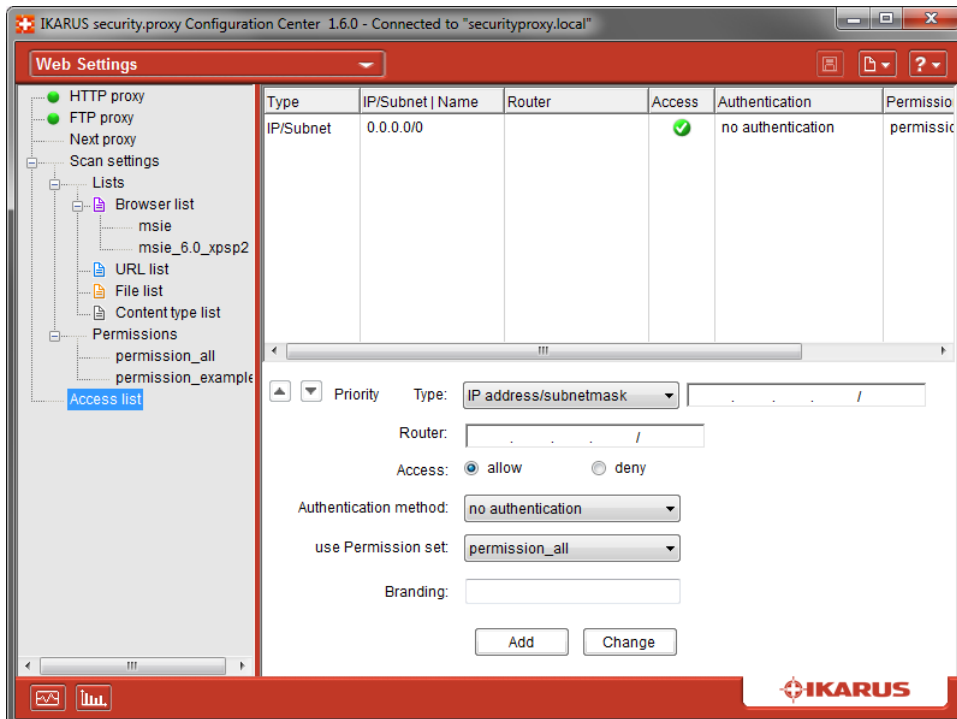


Figure 61: Setting Access list

## 4.6.2 How to Set up a Permission Set

Follow the steps below to allow or deny URLs, files, content types, and browsers:

1. Create a new list of the appropriate type.

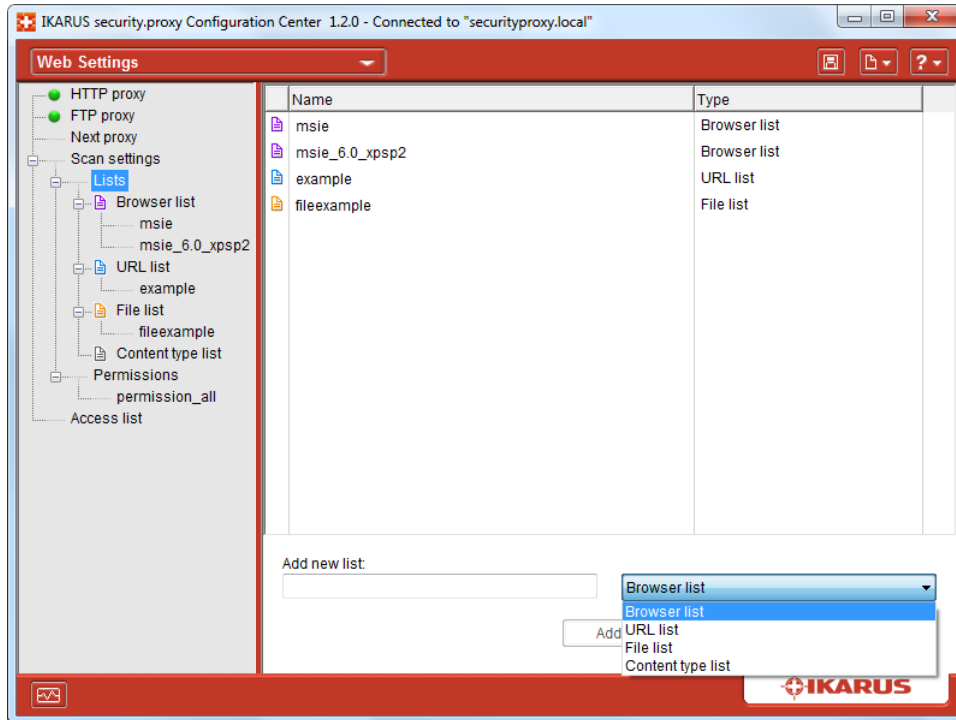


Figure 62: Configure permission set

2. Fill in the required information (e.g. URLs).



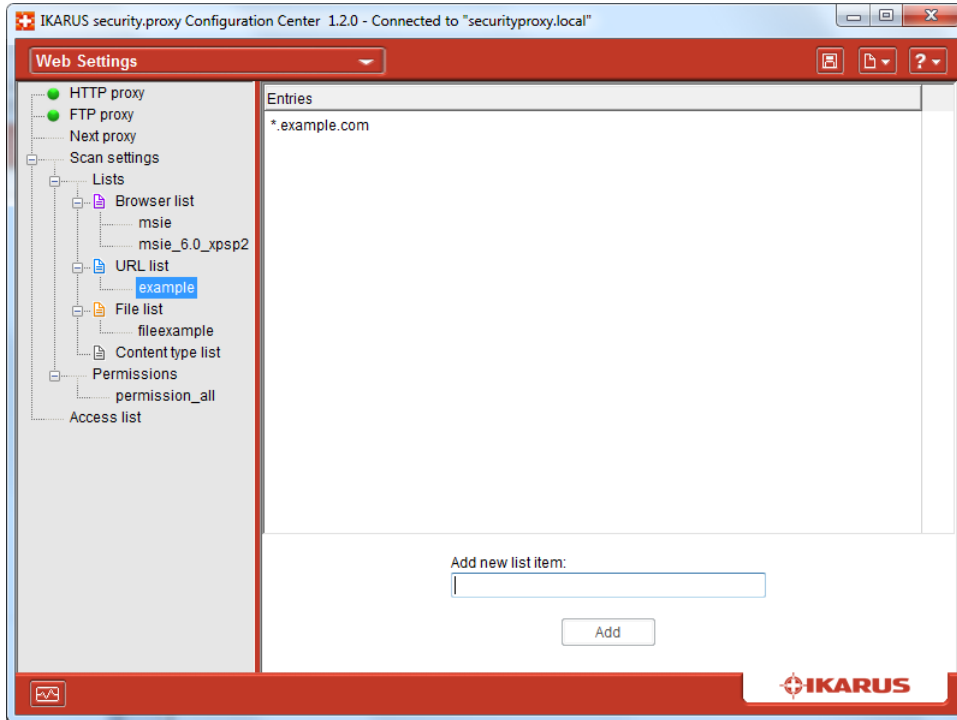


Figure 63: Configure URL list

3. Add the list to your permission set.

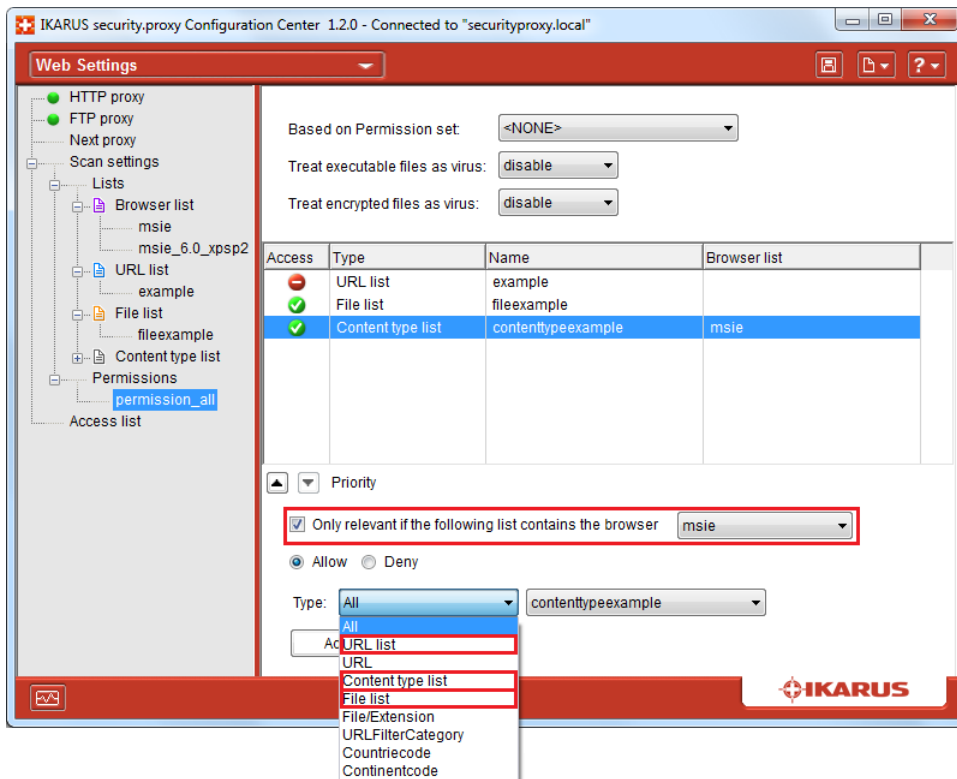


Figure 64: Use URL list in permission set

You may also add URLs and files directly to your permission set:

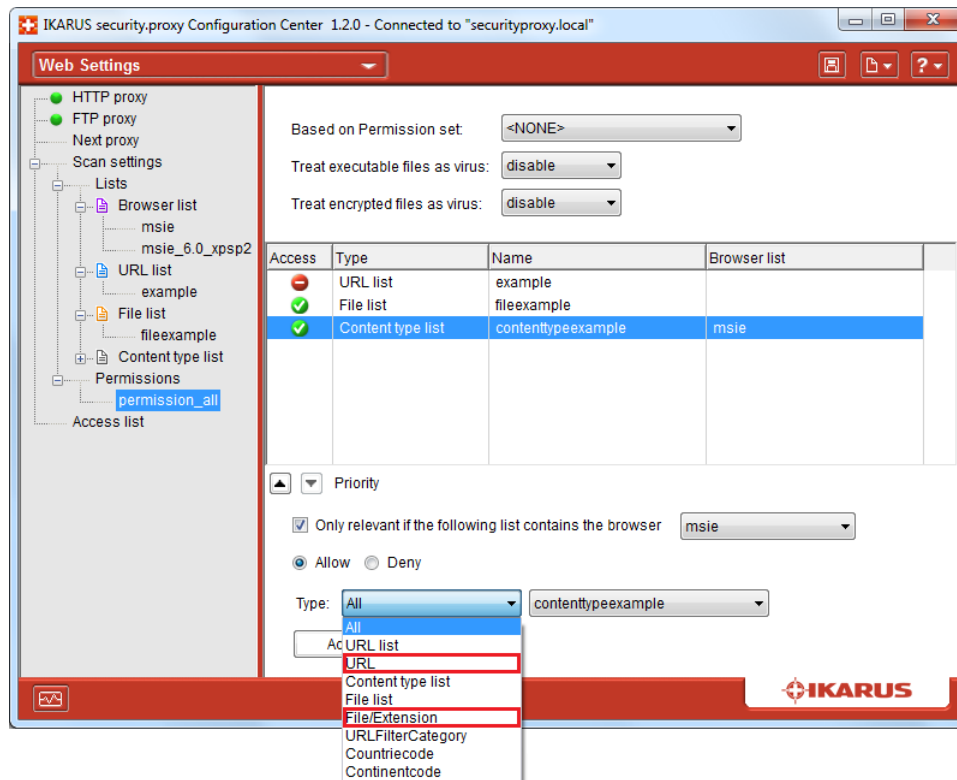


Figure 65: Use URLs/files in permission sets

### 4.6.3 How to Allow or Deny Specific Pages, Domains, or URLs

This section explains how to specify URLs and domains.

- To specify a domain:  
www.example.com
- To specify a domain and all its subdomains:  
.example.com
- To specify only the subdomains of a domain:  
\*.example.com
- To specify a URL and all its sub URLs:  
www.example.com/example

Follow the instructions in section 4.6.2 using this notation technique.

### 4.6.4 How to Allow or Deny Specific Files

Follow the instructions in the section 4.6.2 above.

#### 4.6.5 How to Allow or Deny Specific Contents

Follow the instructions in the section 4.6.2 above.

#### 4.6.6 What is the Purpose of Browser Lists?

Using browser lists, you can allow or deny global Internet access (or access to specific URLs) from specific web browsers. This functionality allows for controlling the web pages that can be accessed from a specific browser.

##### How to use this feature

Create a new list as described in the section 4.6.2 above, and then enter the user-agent string of the desired browser.

For example, you could implement the following security settings:

- A non-Microsoft browser (Mozilla Firefox, Opera) is required for accessing any web pages.
- However, since Microsoft requires the use of the Internet Explorer for accessing Microsoft Updates, you may add an appropriate exception.
- The banking website of your organization's bank is not displayed properly in one of the non-Microsoft browsers. Therefore, you may allow access to the banking pages using the Internet Explorer.
- Access to any other URLs is allowed using non-Microsoft browsers only.

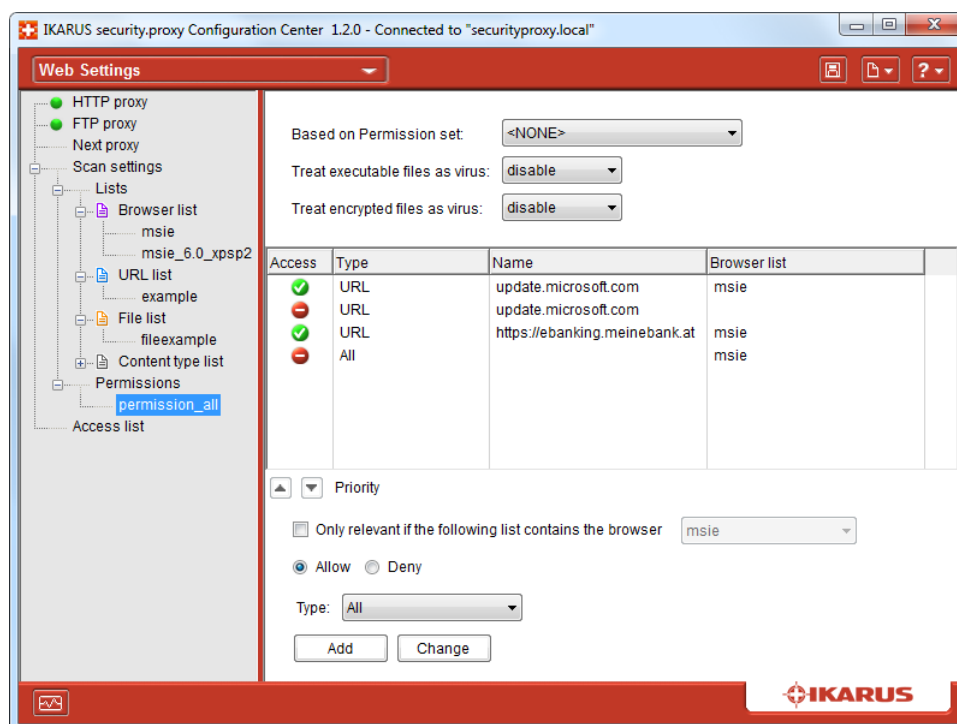


Figure 66: Configure Browser list

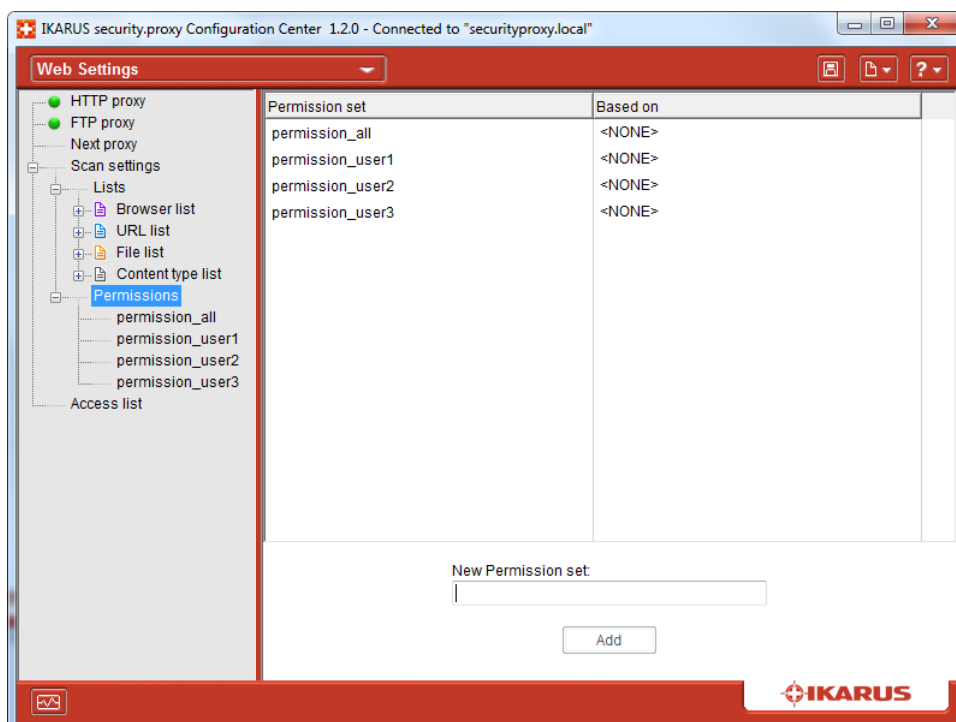
#### 4.6.7 How to Use the Permission Set Properly

You assign the permission set with IP addresses or a network group using the Access List dialog.

1. Select the IP range or network group from the Type list.
2. Enable the Allow option.
3. Choose the appropriate authentication type.
  - (a) No Authentication (i.e. no password protection for the Internet access)
  - (b) Proxy Internal Authentication (uses the **IKARUS security.proxy** internal user administration)
  - (c) LDAP Authentication (uses Active Directory users)
  - (d) NTLM/Kerberos Authentication (uses Active Directory users)
4. Select the permission set to be used, or enter a permission-set mask.
5. Click the Add button.

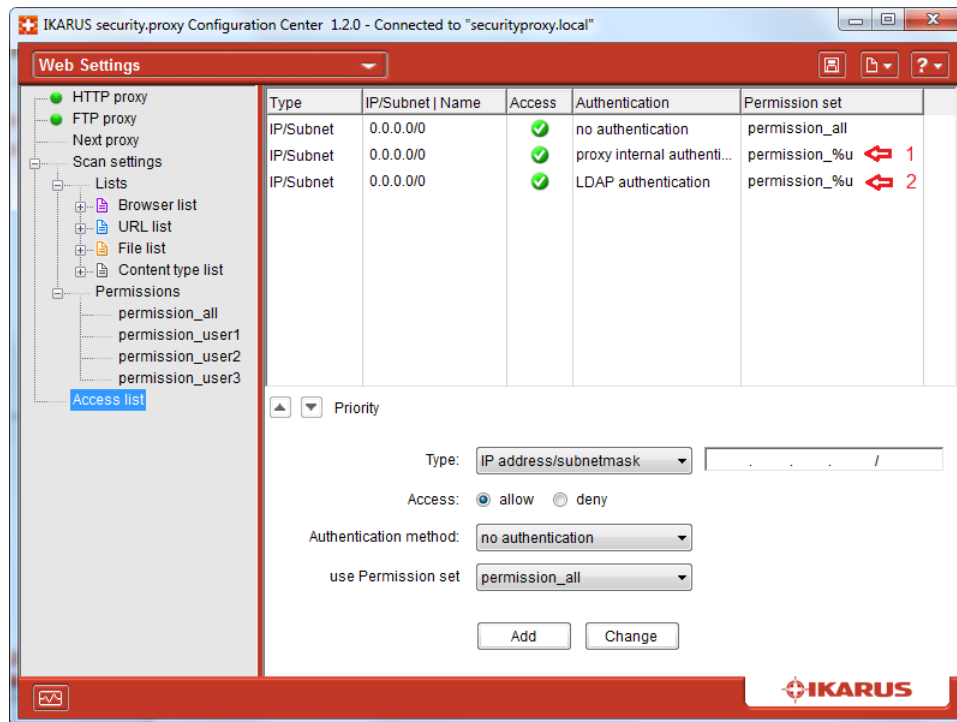
#### 4.6.8 How to Use the Custom Permission Sets

Let us suppose you have created one permission set for each of a number of users. The usernames are "user1", "user2", and "user3".



**Figure 67:** Custom Permission Sets

The access-list entry should look like this:



**Figure 68:** Configure permission set

1. Select Proxy Internal Authentication when you have defined passwords for your permission sets (**IKARUS security.proxy** user administration).
2. Select LDAP Authentication when using Active Directory or a similar directory service with domain users and passwords.
3. Select NTLM/Kerberos Authentication when using Active Directory or a similar directory service with Kerberos tickets.

Be sure to replace %u with the appropriate user name in the Permission Set column.

## 4.7 Greylisting

The term *greylisting* denotes a method for detecting mail transfer agents (MTAs) who are used for delivering spam e-mails. Mail traffic will only be forwarded, if the MTA passes the greylisting check.

Trustworthy MTAs are expected to work according to RFC821. This means that the sender tries to resend e-mails within a certain time span in case they are rejected by the receiver.

If an MTA can be regarded as trustworthy, its IP address can optionally be added to a temporary whitelist.

Besides that there also exists a permanent whitelist. MTAs having their IP address on this list will not have to pass the greylisting check. Their traffic will be forwarded instead.

If temporary whitelisting is enabled, the sender's IP address will be added to this list if the connection has passed the greylisting check. So, traffic from this IP address will also be forwarded for a certain period of time.

**Remark:** Temporary whitelisting is enabled if the period of time mentioned above is set to a value greater than zero (see 3.10.2 ).

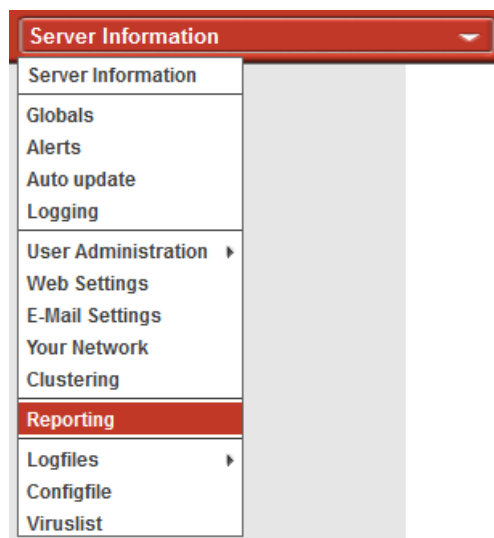
After this period has expired, the MTA has to pass the greylisting check again to be added to the temporary whitelist.

## 4.8 Reporting

IKARUS security.proxy supports creating reports on your e-mail and web activities. Use the **IKARUS security.proxy Configuration Center** for creating and viewing those reports.

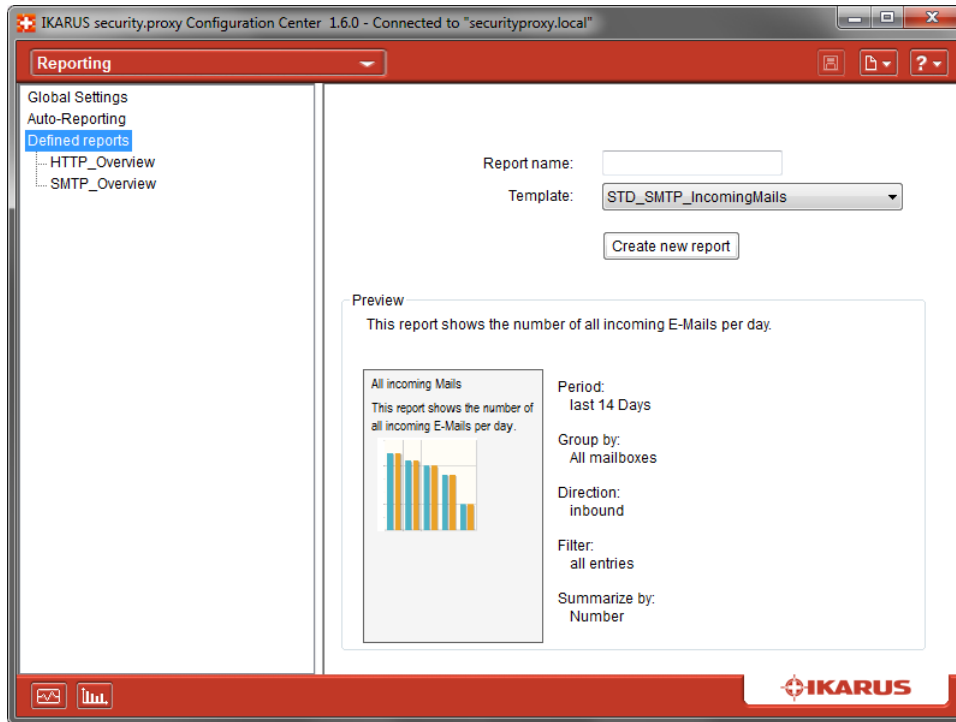
### 4.8.1 How to Create a Report

1. Launch the **IKARUS security.proxy Configuration Center** and select the "Reporting" item from the menu.



**Figure 69:** Reporting menu

2. Next, select the "Defined Reports" item, then choose a template from the list. This template will be the basis of your report. The preview area below the template list will show the default settings of the selected template.



**Figure 70:** Reporting: New report

3. Enter a name for your new report, then click the "Create New Report" button.

#### 4.8.2 How to Edit a Report

1. Select the report to be edited from the tree on the left. This will display the report settings on the right.

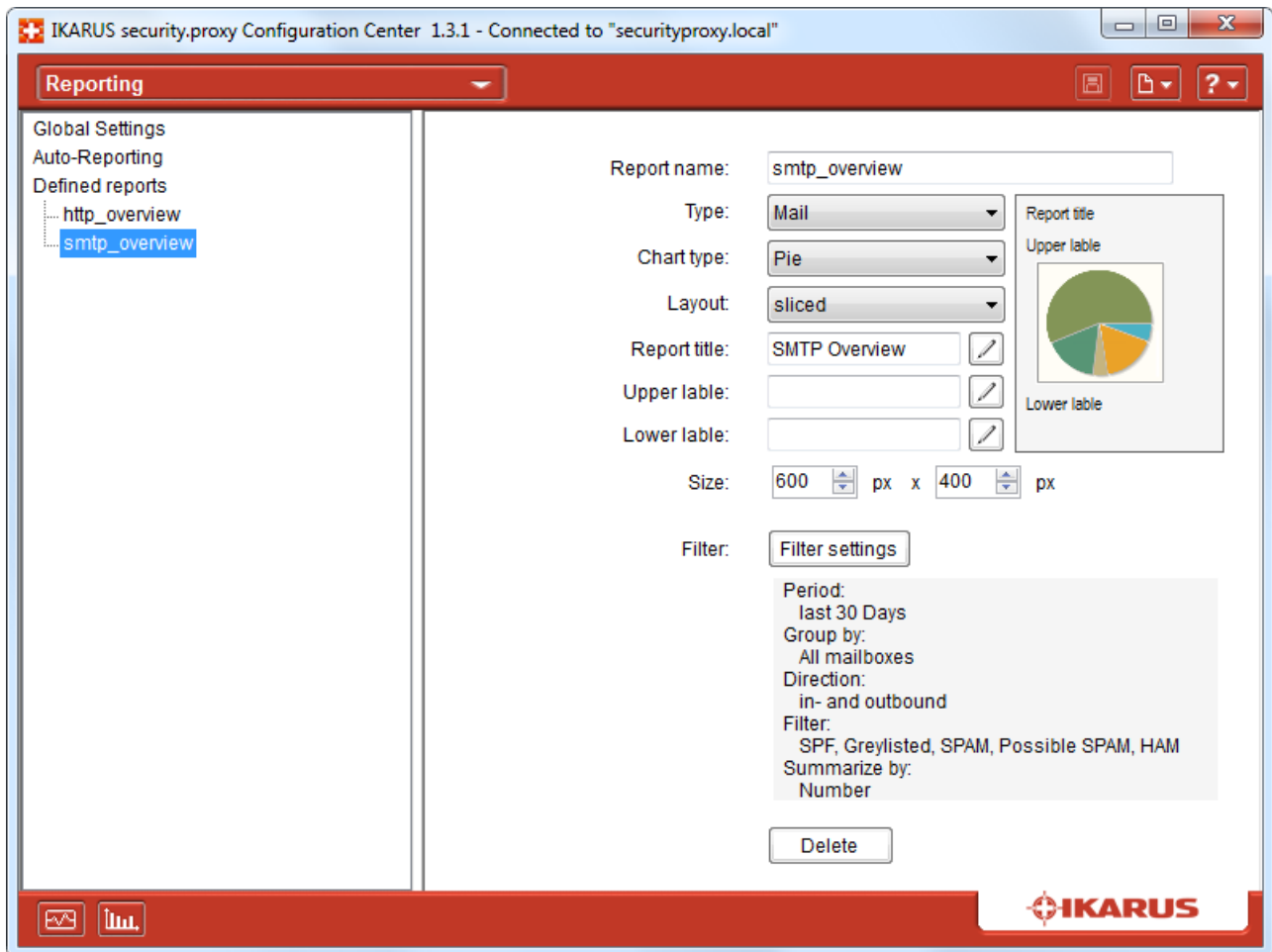


Figure 71: Reporting: Edit

2. Settings that can be changed include:

- the report type
- the chart type (bar, pie, or line chart)
- the report title plus any explanations or additional texts
- the chart size

3. Use the "Filter Settings" button to configure what exactly the report will display. Refer to chapter Reporting for information on the various fields.

4. When your edits are complete, store your report.

### 4.8.3 How to View a Report

Launch the report-view dialog.



Select the desired report from the list, then click the "Show Report" button. The report will be generated and be displayed.



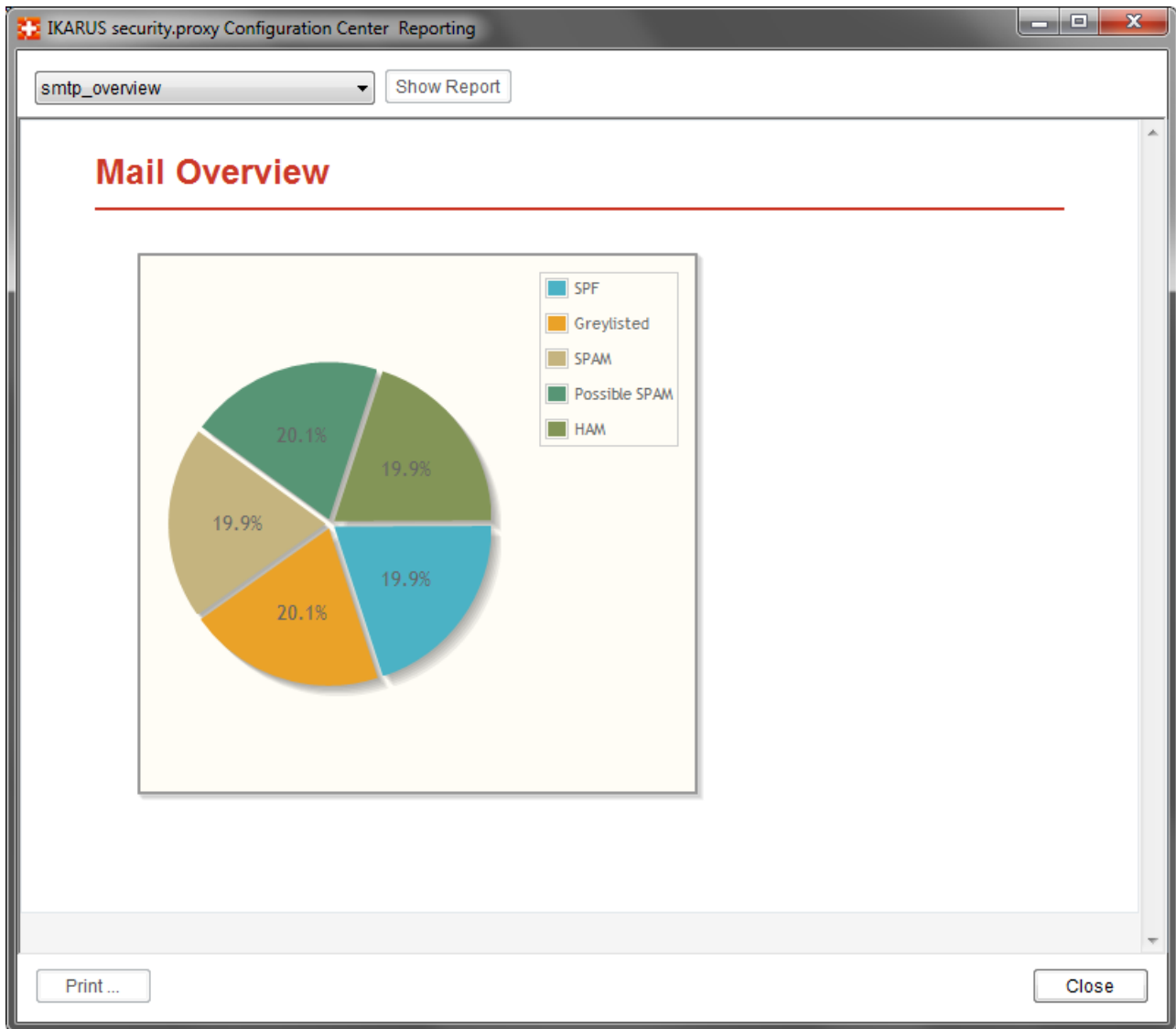


Figure 72: Reporting: Show

#### 4.8.4 How to Send a Report automatically

Select "Auto-Reporting" from the tree on the left. Here you can define, when to send which reports to whom at what given time.

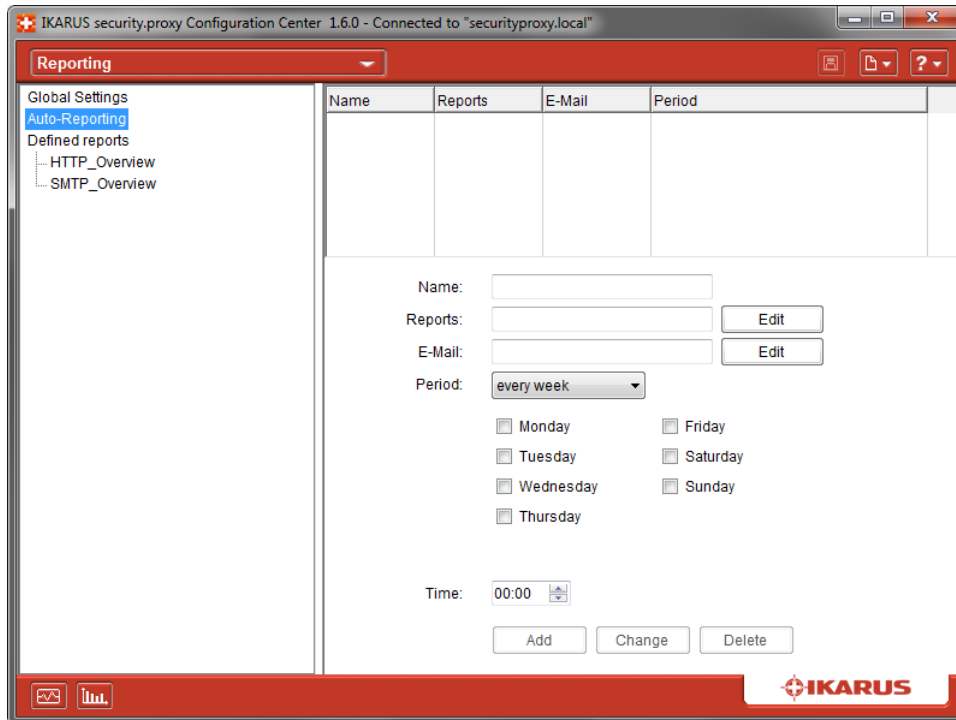


Figure 73: Reporting: Auto-Reporting

1. First enter a name for the Auto-Reporting entry.
2. Then select reports for this entry by clicking on the "Edit" button next to the "Reports" text box.
3. Enter the recipients in the next step by clicking on the "Edit" button next to the "E-Mail" text box.
4. Choose the days of a week or the days of a month at which reports shall be generated and sent.
5. Furthermore select the time of the day for the report creation and delivery. The best choice is a time with low load on the **IKARUS security.proxy** (for example in the middle of the night).
6. Finally add the entry by clicking on the "Add" button and save the configuration. From now on the selected reports will be created and sent to the chosen recipients on selected days at a certain time.

## 5 IKARUS security.proxy FAQ

- ***I cannot install IKARUS security.proxy on a Microsoft Windows system.***  
Make sure to use the correct setup package for your platform. In addition, you need administrative rights on the target system. There are setup executables for 32-bit and 64-bit systems.
- ***I cannot install IKARUS security.proxy on a Linux system.***  
Make sure to use the correct setup package for your platform. In addition, you need administrative rights on the target system. There are setup executables for 32-bit and 64-bit systems.
- ***I cannot connect from the Management Console to IKARUS security.proxy.***  
Verify that the **IKARUS security.proxy** service is running. Make sure that the TCP ports have been properly assigned. The HTTP port defaults to 8080 and the remote-management port to 15639. Confirm that your firewall does not prevent access.
- ***After launching, the IKARUS security.proxy service appears not to run.***  
Check the `splogfile.log` file in the **IKARUS security.proxy** "log" directory to ensure that the service has started correctly. Installing **IKARUS security.proxy** on a system where other services (such as proxies, mail-relay agents, etc.) exist may result in port conflicts. This means that a TCP port assigned during the **IKARUS security.proxy** installation may conflict with an existing port, or may later conflict with a subsequently assigned port. Conflicts prevent assigning the appropriate TCP port to the **IKARUS security.proxy** service. Search the above log file for relevant error messages.
- ***IKARUS security.proxy does not start update processes and does not receive updates. In addition, I cannot connect to the Internet over the proxy.***  
Depending on the settings, **IKARUS security.proxy** may require appropriate Internet access. This is because **IKARUS security.proxy** acts as a proxy, i.e. it receives data coming in from the Internet on behalf of the system. Update files take the same path – they arrive from the Internet in HTTP format. Therefore, it is important to allow the server to send a number of protocols from inside the firewall to the Internet. Protocols required by the application include all of the following: HTTP, FTP, HTTPS, POP3, IMAP, and NNTP. In addition, DNS servers must be entered on the system before installing **IKARUS security.proxy**. This means that the firewall must allow DNS lookups issued by the system.
- ***When calling a web page, a message is displayed that the license has expired or is invalid.***  
The license either has expired or has not yet been added. Add the license using the Management Console or the command line.
- ***How can I ensure that I use IKARUS security.proxy with gateway-antivirus features for Internet access?***  
Be sure to make the appropriate proxy settings in your web client (for example, Microsoft Internet Explorer, Mozilla Firefox, Opera, Google Chrome, or Safari). In addition, always use the port indicated in the HTTP-proxy portion of **IKARUS security.proxy** for web browsing.
- ***Does IKARUS security.proxy support retrieving web pages encrypted using HTTPS?***  
Yes. Again, use the HTTP-proxy port for this purpose. **IKARUS security.proxy** tunnels the HTTPS stream to the target system. Note that content filtering and virus protection are not available for encrypted client/server connections; therefore, you need to make sure that the client runs a local antivirus solution; for example, the **IKARUS anti.virus** endpoint solution.

- ***Can encrypted (HTTPS) traffic be checked for malicious contents?***

This requires the use of additional configuration settings and optional software components. Please contact **IKARUS** if you want to secure HTTPS traffic.

- ***Can Microsoft Internet Explorer be used for accessing an FTP server?***

Yes. Make sure you have defined the HTTP proxy settings of **IKARUS security.proxy** in for HTTP and FTP connections from Internet Explorer. Next, access the FTP server using an appropriate link (for example, ftp://ftp.example.org/). You might then be prompted to enter your user ID and password to authenticate to the FTP server.

- ***Can I reset the password for the user ROOT?***

Yes. Passwords are encrypted and stored on the **IKARUS security.proxy** server in the file `conf\passwd`. If the line starting with `root:` is deleted in this file, the root user can log on again using the default password "root". **Important:** It is up to the system administrator to restrict access to the server's file system. After the password is reset, it must be changed as soon as possible.

## 6 Glossary

Term	Description
<b>IKARUS</b> AntiSPAM Engine	The <b>IKARUS</b> AntiSPAM Engine uses the AntiSPAM database to verify whether incoming messages are spam.
AntiSPAM database (SDB)	<b>IKARUS</b> automatically forward their AntiSPAM database to the SIS Scan Center. The <b>IKARUS</b> AntiSPAM Engine uses the database for differentiating between spam and non-spam.
<b>IKARUS</b> Scan Engine	The <b>IKARUS</b> Scan Engine checks incoming traffic for malicious contents.
Virus database (VDB)	The <b>IKARUS</b> Scan Engine uses the VDB as a source of information on known malware.
Proxy	A service acting as an intermediary for requests from clients seeking resources from remote sources
SSL	Secure Socket Layer
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol using SSL encryption
SMTP	Simple Mail Transfer Protocol
POP3	Post Office Protocol 3
IMAP	Internet Message Access Protocol
NNTP	Network News Transfer Protocol

**Table 40:** Glossary

©2013 **IKARUS Security Software GmbH**. All rights reserved.

The information contained in this document represents the current view of IKARUS Security Software GmbH on the issues discussed as of the date of publication. Because IKARUS Security Software GmbH must respond to changing market conditions, it should not be interpreted to be a commitment on the part of IKARUS Security Software GmbH, and IKARUS cannot guarantee the accuracy of any information presented after the date of publication. This paper is for informational purposes only. IKARUS Security Software GmbH MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. Other product and company names mentioned herein may be the trademarks of their respective owners.

**IKARUS Security Software GmbH** · Blechturmstraße 11 · 1050 Vienna · Austria