Cyclope Internet Filtering Proxy

- User Guide -

Cyclope-Series
- 2010 -

Table of contents

1. Overview

Cyclope Internet Filtering Proxy monitors the entire Internet traffic and blocks the access to websites and files according to the chosen filter. The requested web pages are displayed only if they comply with the specified filters.

Cyclope Internet Filtering Proxy comes to help companies better manage Internet usage and bandwidth consumption, reduce web browsing for personal use during working hours, eliminate explicit content websites form being accessed, protect the network against online threats, and discourage the download of unlicensed software and other copyrighted materials.

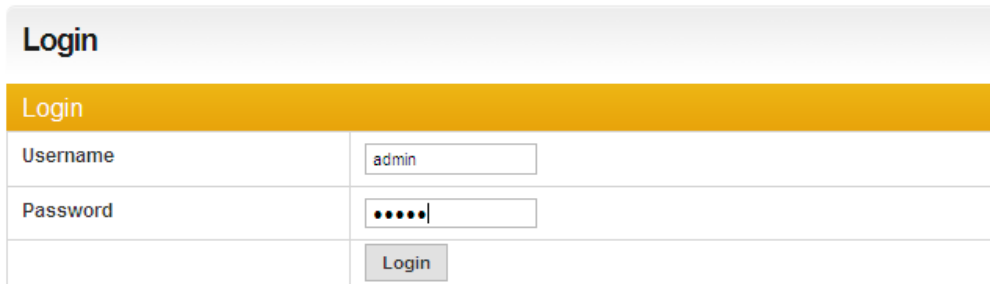Cyclope Internet Filtering Proxy monitors the entire Internet traffic and blocks the access to websites and files according to the chosen filter. The requested web pages are displayed only if they comply with the specified filters.

Cyclope Internet Filtering Proxy is also an Internet Sharing Software, capable of providing cost effective Internet access to multiple computers via a single Internet connection.

2. Cyclope Internet Filtering Proxy User Interface

2.1.   Login

The application web interface is available accessing: web.filter on your browser. For the moment, the interface supports only Internet Explorer browser.

Login

Login	
Username	admin
Password	•••••
	Login

Default login details for the Administrator account are:
- Username: admin
- Password: admin

Default login details for the User account are:
- Username: user
- Password: user

All these details can be changed / modified once you are logged in form the Administration/Account panel.

2.2.   Logout

For logging out, press the Logout button on the right upper corner of the interface.

3. Administration

3.1.   User Management

In the administration field, the application administrator sets the machines to be monitored. The monitored machines are available in an IP list containing IP addresses, user names and computer names.

Monitored Users			
IP Address	Username	Computer Name	
192.168.1.108	guest at 192.168.1.108	192.168.1.108	⊖ Delete
192.168.1.103	guest at 192.168.1.103	192.168.1.103	⊖ Delete

Loging Options	
Option	Status
☑ Log user traffic	✔ Enabled
☑ Log filter activity	✔ Enabled

Adding an IP

In order to filter the Internet traffic on other machines you have to configure their proxy settings to use our product as proxy server. The settings for all browsers installed on client machines should be changed.

After you changed the proxy settings we recommend you to load a few web pages and see if they are loading correctly. If so, the client configuration is completed and you will be able to see the IP addresses of the client machines in the table above.

Deleting an IP

In order to delete an IP address we recommend you to change the proxy server settings on the specific machines. If the proxy settings are not modified the IP address will be added into the list again.

Important note: In order to filter the Internet traffic on other machines you have to configure their proxy settings to use our product as proxy server. The settings for all browsers installed on client machines should be changed (use as proxy server IP 10.0.0.199 and port 8080).

In order to have the **user name** and the **computer name** included in the statistics, **Cyclope Client must be installed on each workstation**. Otherwise, only computer's IP will be provided. This is highly recommended for networks where a

Logging options

This division allows the application's administrator to choose whether he/she wants to log the user's traffic and activity or not.

By enabling the **Log user traffic** option, the Statistics Section will display the traffic report of the users, specifying the resources accessed by the computer and their size. If this option is disabled the traffic report will not display this information.

By enabling the **Log filter activity** option, the Statistics section will display the **Filter activity** report containing the breaking rules attempts. If this option is disabled the Filter activity report will not display this information.

3.2.   Proxy Forwarding

If you already have an http proxy server that shares the Internet Connection in your LAN you can configure our product to forward the http requests to that proxy.

You have to enter the **IP address** and the **Port** of the existing http proxy and check the "I have an existing Http Proxy" option in order to configure our product to forward all the web requests received by our product to the already existing proxy. Our product will do the filtering part before sending the requests to the existing proxy server or after receiving the content from the existing proxy server (before sending the content to the final client). By using this feature our product filtering capabilities remain unchanged.

If you do not have an existing proxy server please do not use this feature by checking options or filling data.

3.3.   Custom error pages

This section allows administrators to customize the error pages sent to the users when they access a blocked resource.

The error pages available are:

Block url error page – the user is displayed this page when is trying to load a blocked website

Block file download error page – the user is displayed this page when is trying to download a file with an unauthorized extension

Block keyword content error page - the user is displayed this page when is trying to load forbidden content

Traffic size error page - the user is displayed this page when the maximum daily traffic allowed is exceeded.

After you select the error page you want to customize press **Preview** in order to preview changes and **Save** in order to save the page

3.4.   Accounts

This field contains the registration details, the login information and the e-mail reporting settings.

There are two types of accounts:
- Administrator account
- User account

When you are logged as an **Administrator** there are **no restriction** regarding the functionality of Cyclope Internet Filtering Proxy.

The **User** account allows **only the viewing** of the Cyclope Internet Filtering Proxy Statistics section.

Account

Registered

Name:	Not registered 13 days left
Number of Computers:	
Expires:	

Change Password

Account Type:	⦿ Administrator ○ User
Type Password:	
Retype Password:	
	Change Password

Email Reporting

Configure E-mail Reporting	Configure

Default login information for the Administrator account is:
Username: admin
Password: admin

Default login information for the User account is:
Username: user
Password: user

Change password

- Please choose the account type (Administration or User)
- New Password
- Retype Password

Note: Only the login password can be changed for users and administrators. The login names that are allowed by our product are admin and user – no new logins can be created.

In this section the administrator is allowed to configure the e-mail reporting settings in order to receive the reports generated by Cyclope Internet Filtering Proxy to a specified e-mail address.

3.5.   Backup-Restore

Allows you to backup / restore your settings. This feature is useful for companies that have multiple instances of Cyclope Internet Filtering Proxy installed, in order to have the settings (filtering policy) on all servers.

You can check which settings will be included in the backup:

- **Web Sites** (which websites are blocked and which are allowed; black list and white list)
- **Keywords & Profiles** (the list of blocked words and the profiles)
- **Files & Extensions** (the list of file types that are blocked)
- **Scheduler for the Filters** (if you have defined a scheduler for the filtering policy this can be included in the backup)
- **Rules** for each IP (the list of IP addressed that are excluded from the filtering policy)
- **Groups** (the group structure that you have defined)
- **Passwords** (user and admin passwords can be included in the backup).

When **Backup** Button is pressed, a zip file is created and stored into the application folder (usually c:\Program Files\CIFP). The zip file name is CIFPBackup_month_day_year.zip (example CIFPBackup_07_19_2007.zip).

When **Restore** button is pressed you will be able to select a zip file (named CIFPBackup_month_day_year.zip) from the installation folder (usually c:\Program Files\CIFP) which will be used to restore the settings. **Please note that the RESTORE will overwrite the existing settings with the settings (filtering policy, ip rules, passwords) stored in the backup file**.

Backup-Restore

Backup Data	
Web Sites	☐
Keywords / Profiles	☐
Files / Extensions	☐
Scheduler for the Filters	☐
Rules for each IP	☐
Groups	☐
Passwords	☐

Backup File	Options
[ ] Browse...	🔶 Backup 🔼 Restore

4. Filter Configuration

Cyclope Internet Filtering Proxy allows multiple filters enabling for increased network protection. Filters can be a specific web page, a keyword, a group of letters, and an extension or file type.

The Filter Configuration section allows you to configure the filters, to monitor their status and to manage the different groups.
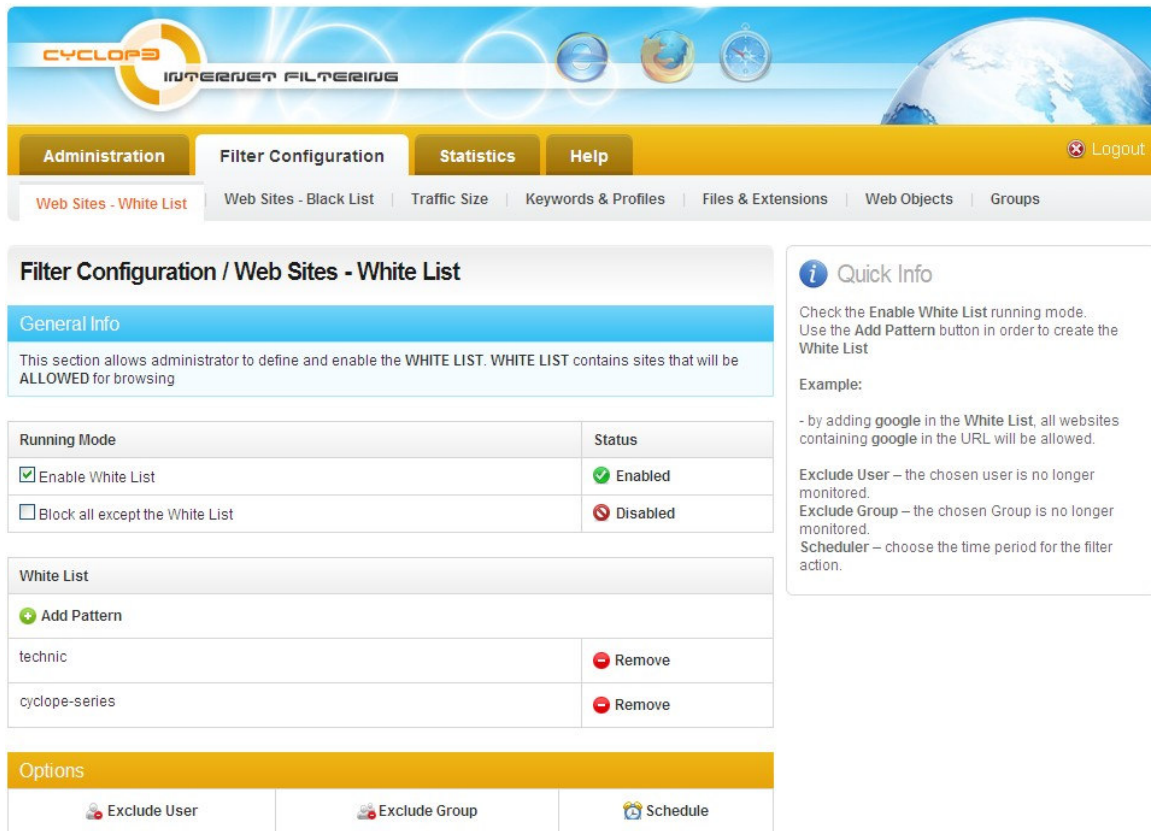
The divisions of this section are:

1. **Web Sites - White list** - allow defining accepted websites for browsing.
2. **Web Sites - Black list** - blocks URL from being displayed.
3. **Traffic size** - blocks Internet access when the specified traffic size is exceeded
4. **Keywords & Profiles**- blocks a web page containing a specified word from being displayed.
5. **Files & Extensions**- blocks access to different file types (archives, applications, audio-video, etc.)
6. **Web Objects** - Block Shockwave and Flash objects from running, incoming cookies from being set on your computer and outgoing cookies from being read from your computer.
7. **Groups (Group Management)** – allows the application administrator to create different groups of users.

4.1.   Web Sites-White list:

This filter blocks access to a specified web site or all web sites.

Block all except the **White list**

In the **Web Sites - White list** section, by defining and enabling the White list, the user will be authorized to browse the websites added in the White list no matter what other restrictions might have been set. The **Add Pattern** option assures you that all websites containing the specified pattern will be allowed (like groups.google.com not only google.com).

4.2.   Web sites - Black list

This filter blocks access to a specified web site or all web sites.

In the **Web Sites - Black List** section, by defining and enabling the Black List, the websites added in the Black List will be blocked. The **Add Pattern** option assures you that all websites containing the specified pattern will be blocked (like groups.google.com not only google.com).

Options:

For better property management, after you add the websites, there is the **Remove** option.

- **Exclude User** – That user is no longer monitored. Pressing the Exclude user button will lead you to a new window. Choose the user you want to exclude than press Change to validate your request.
- **Exclude Group** – The chosen group of users is no longer monitored. Pressing the Exclude Group button will lead you to a new window. Choose the group you want to exclude than press Change to validate your request.
- **Scheduler** – removes IPs for a specified period of time from the filter action. To schedule filter activity, press the Scheduler button and chose the period when you want the filter to be inactive.

The user will see the following message:

Note: For information about building custom error / blocked access pages go to Administration / Custom error pages section.

4.3.   Traffic size

This section allows administrator to define maximum daily traffic allowed for each monitored user. After entering the maximum daily traffic allowed, press Change to save changes for each user.

Example:

By entering 100 in the corresponding field, after 100 MB of traffic the user will be prompted that the maximum traffic allowed has been exceeded and no more browsing will be allowed.

By leaving the field (unlimited) for a specific user there will be no restrictions for that specific user.

4.4.   Keywords & Profiles

For enhanced protection, Cyclope Internet Filtering Proxy has a keyword filter, meaning that it stops web pages containing in their body a specified word or a group of letters from being displayed.

In the **Keywords & Profiles** filter section you can choose to create your own **Custom Word List** and/or to use the **predefined profiles** provided by Cyclope Internet Filtering Proxy.

- If you choose to define your own, **custom word list** use the **Add Word** button in order to create the block list. When the keyword is found in the

website body, that website will be replace with a page containing restriction details.

The **Add non-english word** option, included in this filter, allows blocking the access to non-english web sites as well. The web sites containing the specified non-english word will not be displayed.

Filter Configuration / Keywords & Profiles

Options

New word	
Character set	⦿ Arabic ○ Baltic ○ Central European ○ Chyrillic ○ Greek ○ Hebrew ○ Latin ○ Thai ○ Turkish ○ Vietnam

⊕ Add Word

Word List

Word	Character set	
τυχερά	Greek	⊖ Remove
القمار	Arabic	⊖ Remove

When selecting the character set please read the following:

 - select **Chirillic** for Razeri, Belarusian, Bulgarian, FYRO Macedonian, Kazakh, Kyrgyz, Mongolian, Russian, Serbian, Tatar, Ukrainian, Uzbek, and Macedonian;
- select **Latin** for Afrikaans, Basque, Danish, Dutch, Faroese, Finnish, French, German, Icelandic, Irish, Italian, Malay, Norwegian, Portuguese, Scottish, Spanish, Swedish, Swahili;
- select **Central European** for Albanian, Croatian, Czech, Hungarian, Polish, Romanian, Serbian (Latin), Slovak, Slovenian;
- select **Baltic** for Lithuanian, Latvian, Estonian;
- select **Arabic** for Arabic, Farsi, Urdu.

- If you choose the **predefined profiles** provided by **Cyclope Internet Filtering Proxy**, check the appropriate profile in order to enable it.

For better property management, in case of changes in the word pattern contained in the sites to block you can access the **Remove** option.

The user will see the following message:

! Cyclope Internet Filtering Proxy

You are not allowed to view the content of this page.

Please contact your System Administrator for more information.

Options:

• **Exclude user** – the chosen user is no longer monitored.
• **Exclude Group** – the chosen Group is no longer monitored.
• **Scheduler** – choose the time period for the filter action.

4.5.   Files & Extensions

In the **Files & Extensions** filter section you can choose to create your own **Custom Extensions List** and/or to use the already **defined extensions** provided by Cyclope Internet Filtering Proxy.

- If you choose to define your own, **custom extension list** use the **Add** button in order to create the block list.

Filter Configuration / Files & Extensions

General Info

This section allows administrator to BLOCK ACCESS to different file types based on their extensions. The filter allows user to:
1. Add CUSTOM EXTENSIONS
2. Use ALREADY DEFINED EXTENSIONS

Running Mode	Status
☐ Block Custom Extensions	🚫 Disabled
☑ Block Predefined Extensions	✅ Enabled

Custom Extensions	Predefined Extensions	
➕ Add Extension	☑ Archives (zip files)	✅ Enabled
	☑ Archives (rar files)	✅ Enabled
	☑ Archives (ace files)	✅ Enabled
	☑ Executables (exe files)	✅ Enabled
	☑ Executables (bat files)	✅ Enabled
	☑ Media (mp3 files)	✅ Enabled
	☑ Media (wav files)	✅ Enabled
	☑ Media (mpeg files)	✅ Enabled
	☑ Media (avi files)	✅ Enabled
	☑ Media (mpg files)	✅ Enabled

Options

👤 Exclude User	👥 Exclude Group	⏰ Schedule

Note: When a new extension is added – pdf for example you have to fill just the extension name (pdf). Using other combinations like .pdf or *.pdf is not supported and as result the access will not be blocked to the resources.

When blocking that type of file, the link will be redirected to an error page informing the blocked access to that specific file.

The user will see the following message:

Cyclope Internet Filtering Proxy

You are not allowed to download this file.

Please contact your System Administrator for more information.

For better property management, in case you don't want to block an extension anymore, use the **Remove** option.

- If you choose the **predefined extensions** as a Running Mode, please check the appropriate extension in order to enable the filter.

According to the chosen extension, the archive files, the applications and the audio-video files will be stop from being downloaded.

Options:

● **Exclude user** – the chosen user is no longer monitored.
● **Exclude Group** – the chosen Group is no longer monitored.
● **Scheduler** – choose the time period for the filter action.

4.6.   Web Objects

This section allows administrator to stop **Shockwave-Flash Objects** from being run and to stop **Cookies** from being set or read from your LAN Computers.

Filter Configuration / Web Objects

General Info

This section allows user to:
1. Stop SHOCKWAVE-FLASH OBJECTS from being run
2. Stop COOKIES from being set or read from your LAN Computers

Running Mode	Status
☑ Block Shockwave-Flash Objects	✓ Enabled
☑ Block Incoming Cookies	✓ Enabled
☑ Block Outgoing Cookies	✓ Enabled

Block Shockwave-Flash Objects

➕ Add Pattern

Block Incoming Cookies

➕ Add Pattern

Block Shockwave-Flash Options

👤 Exclude User

👥 Exclude Group

⏰ Schedule

Block Incoming Cookies Options

👤 Exclude User

👥 Exclude Group

⏰ Schedule

Block Outgoing Cookies

➕ Add Pattern

Block Outgoing Cookies Options

👤 Exclude User

👥 Exclude Group

⏰ Schedule

In the **Web Objects** filter section there are three Running Modes available:

● **Block Shockwave-Flash Objects** - blocks the display of Shockwave and Flash applications within a web page. The content of the web site is loaded just the flash object is not shown.

- For defining the URL pattern, click **Add Pattern** button then write the letter group contained in websites you would like to block.
- **Add All:** by clicking this button, shockwave-flash objects from all websites will be blocked.

For better property management, the filter provides a **Remove** option.

● **Block Incoming Cookies** – This filter stops cookies from being set on a computer. It can be applied to a specified web page and also on web pages containing a keyword or a group of letters.

Cookies are usually set by web sites that need further user recognition or login details. It is recommended to check the login operation on these websites before blocking the access.

- For defining the URL pattern, click the **Add Pattern** button then write the letter group contained in websites you would like to block.
- **Add All:** by clicking this button, the incoming cookies for **all websites** will be blocked.

For better property management, the filter provides a **Remove** option.

● **Block Outgoing Cookies** – This filter stops cookies from being read from a computer. It can be applied to a specified web page and also on web pages containing a keyword or a group of letters.

Cookies are usually set by web sites that need further user recognition or login details. It is recommended to check the login operation on these websites before blocking the access.

- For defining the URL pattern, click the **Add Pattern** button then write the letter group contained in websites you would like to block.
- **Add All:** by clicking this button, the outgoing cookies for **all websites** will be blocked.

For better property management, the filter provides a **Remove** option.

Options:

● **Exclude user** – the chosen user is no longer monitored.
● **Exclude Group** – the chosen Group is no longer monitored.
● **Scheduler** – choose the time period for the filter action.

4.7. Groups

Group Management allows application manager to create groups for different categories of users.

- **Add Group -** Create a new group for a specific category of users. After you include the computers' IP in each group, you will se a detailed list.
- **Add user -** Assign user to a specified group.
- **Delete Group -** Choose the group you want to delete.
- **Rename Group -** Choose the group you want to rename and enter the new name.
- **Delete Computer -** Delete user/computer from the specified group.
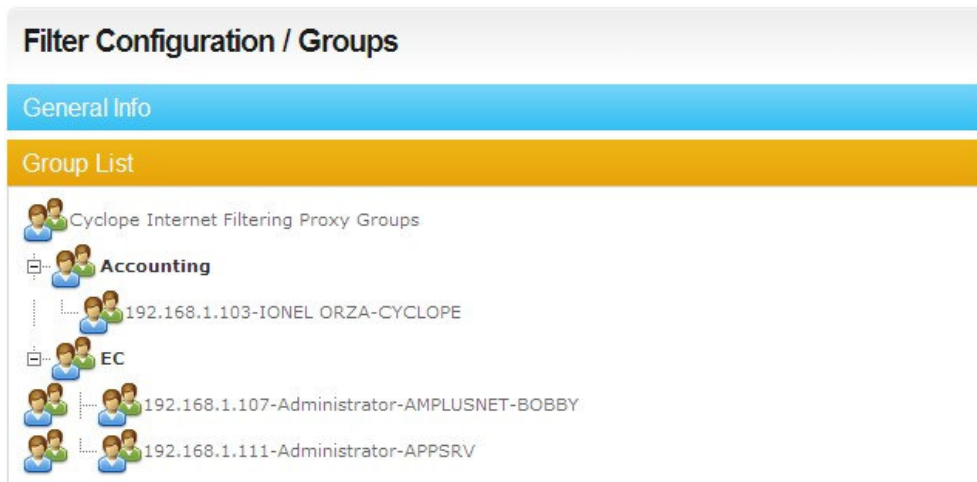
5. Statistics

5.1.   Overview

First time when the administrator runs Cyclope Internet Filtering Proxy, the overview page will guide him to client configuration, to define the filtering policy and to check statistics. Information about the running mode is also available (trial mode or registered).

Overview

Quick Installation Guide

Clients Installation

In order to have the **user name** and the **computer name** included in the statistics, **Cyclope Client** must be installed on each workstation. Otherwise, only computer IP will be provided. This is highly recommended for networks where a **DHCP** server is used. The client application can be installed manually or using the **GPO** domain policy.

Read More

Define Filtering Policy

Cyclope Internet Filtering Proxy allows multiple filters enabling for increased network protection. Filters can be a specific web page, a keyword, a group of letters, and an extension or file type.

Read More

Check Statistics

Traffic & Websites panel reports the user activity and size (expressed in Megabytes - Mb) and chart in traffic.

Read More

Registration

Thank you for using **Cyclope Internet Filtering Proxy**. You are currently running in **trial mode**, and you have **6 days left** from the trial period

Contact

For any questions you might have or in order to provide us your feedback please contact us at support@cyclope-series.com.

Contact us at sales@cyclope-series.com to register your trial copy and to find out the current promotion we are running for Cyclope Internet Filtering Proxy.

The Overview page provides information about:
- o The running mode, trial or registered and the license details like number of users and validity of license.
- o Summary statistics – the number of users currently using the product, the total amount of traffic that was recorded for the current day and the breaking rules attempts.

Overview

Statistics

Today **Cyclope Internet Filtering Proxy**

    has been used by **5 users**

    has recorded a **total traffic size of 4.02 MB**

and here are the breaking rules attempts

    Keyword restriction to web page

Registration

Thank you for using **Cyclope Internet Filtering Proxy**. You are currently running in **trial mode**. and you have **5 days left** from the trial period

Contact

For any questions you might have or in order to provide us your feedback please contact us at support@cyclope-series.com.

Contact us at sales@cyclope-series.com to register your trial copy and to find out the current promotion we are running for **Cyclope Internet Filtering Proxy**.

5.2. Traffic and Websites

Traffic & Website panel reports the IP activity and size (expressed in Megabytes - Mbytes) and chart in traffic. The **View Log** button allows you to see the accessed pages. Below the table, there is the total traffic made on the filtering proxy.
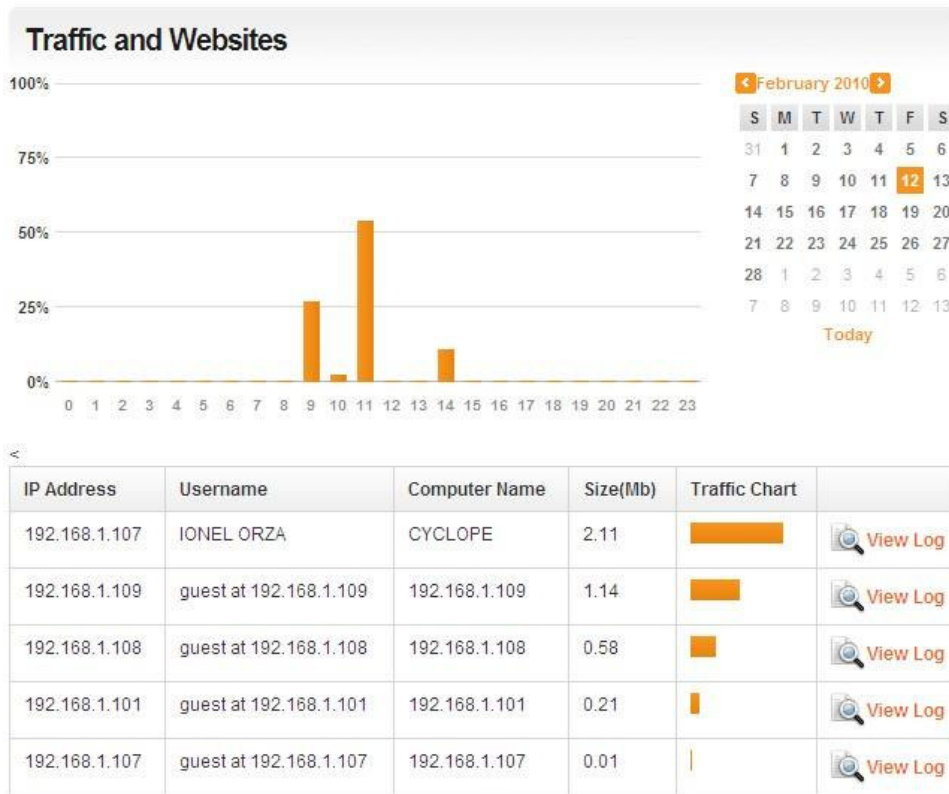
Logs can be visualized on specified dates, choosing the date from the calendar above the table.
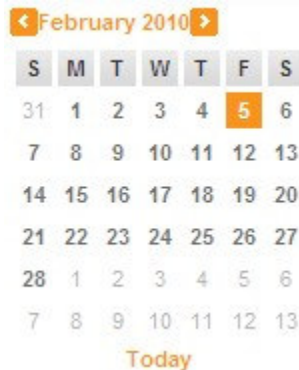
5.3.   Filter Activity

The filter activity panel reports the results of the application usage. Filter activity reporting shows all filter activity and the breaking rules attempts.

The website visited and the action taken by Cyclope Internet Filtering Proxy are presented in a table format, accompanied by information on date, time, IP and computer name Filter action may be: URL blocked, download stopped, and incoming cookies blocked etc. Filter activity reports are available on daily basis.

5.4.   Aggregated Traffic and Websites

Aggregated traffic logs provide detailed information on the traffic made by the monitored IPs for specific periods of time.
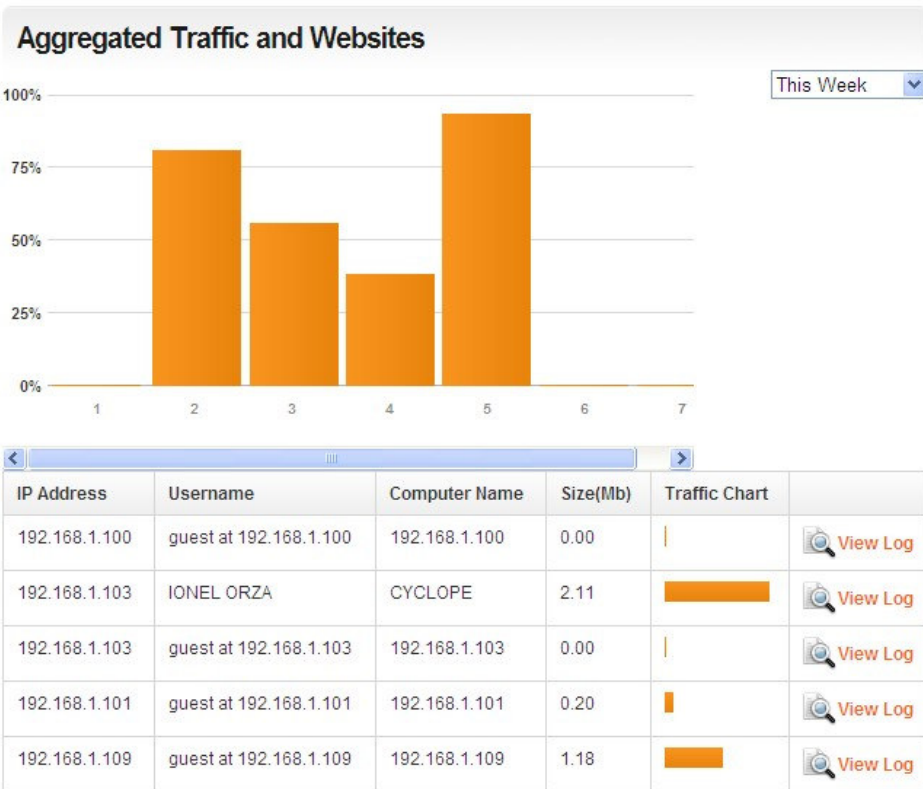
The period of time can be selected from the dropdown list, next to the chart. Time periods can be: this week, last two weeks, last months, last three months, last six months and last year. The table presents the monitored IPs, computers name, traffic size in Kb, and a graphical representation of the traffic made by that IP. Below the table is the total traffic made by the monitored IPs.

5.5. Aggregated Filter Activity

Aggregated Filter Activity logs provide detailed information on the filter activity made for specific periods of time. Filter table shows all active filters; in the case of file extension filters, only active extensions are shown. Aggregated filter activity report can cover specific periods of time, available to be chosen in the drop down list.

Aggregated Filter Activity

Active Filters						This Week
Block Url						
Keyword restriction to web page						
Block incoming cookies						

Time	Date	IP Address	Username	Computer Name	Url	Filter Action
14:21	02/12/2010	192.168.1.108	192.168.1.108	192.168.1.108	http://www.cyclope-s	url
14:21	02/12/2010	192.168.1.108	192.168.1.108	192.168.1.108	http://www.cyclope-s	url
14:21	02/12/2010	192.168.1.108	192.168.1.108	192.168.1.108	http://www.cyclope-s	url
14:21	02/12/2010	192.168.1.108	192.168.1.108	192.168.1.108	http://www.cyclope-s	url

5.6. E-mail Reporting

In the reporting section you have to configure the e-mail reporting settings so that you can receive the reports provided the Cyclope Internet Filtering Proxy solution.

By default the email reporting feature is configured to use our mail server to deliver you the reports. In order to test this feature, please enter your email address in the first field and press Test E-mail button. Check your email and see if you have received an email from cifp@amplusnet.com with the subject Email Reports from Cyclope Internet Filtering Proxy and the attachment: test.zip.

Note:

Other options that can be configured are:
- the sending hour which allows you to specify when the emails should be sent,
- your own email server details:
    - Name – this is the information that will be present in the from field
    - E-mail Address – the email address that will be used for sending the email
    - Authentification Method that is supported by your SMPT server (the most common is AUTH LOGIN)

o User Name – is the SMPT server username (usually is full email address)
o Password – the password for the SMPT server
o Mail Server – the name or the IP address of your SMP server
o Port – the port used by your SMP server (the default value is 25)

- The types of the reports that you will receive by email:
   o Daily Traffic Report – this report will be delivered each day (at the hour that you have previously configured) and will contain the a table with all the IP addresses and the traffic (download and upload) for each of them;
   o Weekly Traffic Report – this report aggregates the daily logs and provides the same data (traffic size for each IP) for a week.
   o Monthly Traffic Report – this report aggregates the weekly logs and provides the same data (traffic size for each IP) for a month.
   o Daily Filter Activity Report – shows a table with the Date, Time, IP Address, Web Site and Filter Type that blocked the user access to a web resource.
   o Weekly Filter Activity Report – aggregates the daily reports into a single report
   o Monthly Filter Activity Report – aggregates the weekly reports into a single report

Use **Save settings** to validate your options.

7. Registration

In order to register your product, please go to:
http://www.cyclope-series.com/internet-filtering/order.html

Before proceeding, make sure that you have disabled the product so that the payment processing service provider web page can be accessed without any restrictions. The license key and registration instructions will be sent by email.

8. Support

E-mail Support
For any technical related question please contact our technical support team: support@cyclope-series.com
For any sales related questions please contact our sales support team: sales@cyclope-series.com

Phone Support
Our phone support lines (available during working days):
+40 365 401269