LANCOM Content Filter Option

- Handbuch
- Manual

LANCOM
Systems

LANCOM Content-Filter

LANCOM
Systems

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

Subject to change without notice. No liability for technical errors or omissions.

Products from LANCOM Systems include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Products from LANCOM Systems include cryptographic software written by Eric Young (eay@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen
Germany

www.lancom.eu

Wuerselen, May 2010

Preface

Thank you for your confidence in us!

The LANCOM Content-Filter acts to filter out Internet websites with undesirable content. It enables you to allow or forbid access to certain website pages and to carry out checks on the content of an online server according to predefined categories.

! The use of the LANCOM Content-Filter Option may in certain countries be subject to certain restrictions by data-privacy laws or directives, and/or to company guidelines. Before activating the LANCOM Content-Filter Option, please be sure to check the relevant laws, directives or agreements.

Security settings

To maximize the security available from your product, we recommend that you undertake all of the security settings (e.g. firewall, encryption, access protection) that were not already activated when you purchased the product. The LANconfig Wizard 'Security Settings' will help you with this task. Further information is also available in the chapter 'Security settings'.

We would additionally like to ask you to refer to our Internet site www.lancom.eu for the latest information about your product and technical developments, and also to download our latest software versions.

This documentation was created by …

... several members of our staff from a variety of departments in order to ensure you the best possible support when using your LANCOM product.

Should you find any errors, or if you would like to suggest improvements, please do not hesitate to send an e-mail directly to:
info@lancom.eu

i Our online services www.lancom.eu are available to you around the clock if you have any questions on the content in this manual, or if you require any further support. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledgebase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.
In addition, LANCOM Support is available. For telephone numbers

and contact addresses for LANCOM Support, please refer to the enclosed leaflet or the LANCOM Systems Web site.

Information symbols	
⚡	Very important instructions. Failure to observe these may result in damage.
❗	Important instruction that should be observed.
ℹ	Additional information that may be helpful but is not essential.

Contents

1 Activating the LANCOM Content-Filter Option 3

1.1 Prerequisites for installation 3

1.1.1 System requirements 3

1.1.2 Package content 3

1.1.3 Configuration computer with the Windows operating system 3

1.1.4 Up-to-date LANconfig 4

1.1.5 Up-to-date firmware in the LANCOM 4

1.2 Online registration 4

1.3 Activating the LANCOM Content-Filter Option 5

1.4 Checking the activation 6

2 Configuring the LANCOM Content Filter 8

2.1 Introduction 8

2.2 Requirements for using the LANCOM Content Filter 10

2.3 Quick start 10

2.4 Default settings in LANCOM Content Filter 11

3 Advanced configuration of the LANCOM Content Filter with LANconfig 14

3.1 General settings 14

3.2 Settings for blocking 17

3.2.1 Block-Text 18

3.2.2 Error-Text 20

3.3 Override settings 21

3.3.1 Override text 23

3.4 Profiles in the LANCOM Content Filter 25

3.4.1 Profiles 25

3.4.2 Blacklist addresses (URL) 28

3.4.3 Whitelist addresses (URL) 29

3.4.4 Category-Profiles 30

3.5 Options with the LANCOM Content Filter 32

3.6 Additional settings for the LANCOM Content Filter 35

3.6.1 Firewall settings for the content filter 35

3.6.2 Timeframe 37

4 Status messages 39

4.1 LANmonitor 39

4.1.1 Information displayed by LANCOM Content Filter in summary 39

4.1.2 Detailed displays in LANCOM Content Filter 40

4.1.3 Functions in LANmonitor 42

4.2 WEBconfig 42

4.2.1 Users 43

4.2.2 Category statistics 43

4.2.3 Last-Snapshot 43

4.2.4 Log 44

4.2.5 Override-Log 44

4.2.6 Cache 45

4.2.7 Performance 46

4.2.8 Proxy connections 47

5 Tutorial: Using multiple content filter profiles 49

1 Activating the LANCOM Content-Filter Option

This brief chapter informs you how to activate the LANCOM Content-Filter Option on your LANCOM. Activation takes place in four steps:

① Ensuring that the prerequisites for installation are fulfilled

② Online registration

③ Entry of the activating code

④ Checking the activation

1.1 Prerequisites for installation

> The use of the LANCOM Content-Filter Option may in certain countries be subject to certain restrictions by data-privacy laws or directives, and/or to company guidelines. Before activating the LANCOM Content-Filter Option, please be sure to check the relevant laws, directives or agreements.

1.1.1 System requirements

Please ensure that you have met all of the requirements to successfully operate the LANCOM Content-Filter Option:

- LANCOM device with the option of activating the LANCOM Content-Filter Option.
- Proof of license for the LANCOM Content-Filter Option.

1.1.2 Package content

Please ensure that the Option package includes the following components:

- Proof of license with a printed license number
- Manual

1.1.3 Configuration computer with the Windows operating system

To install the LANCOM Content-Filter Option with LANconfig, you require a computer with the Windows operating system. Alternatively, activation can be performed via WEBconfig.

The computer must have access to the LANCOM device that is to be configured. Access may be via the LAN or via remote access.

1.1.4 Up-to-date LANconfig

The latest version of LANconfig and LANmonitor are available for download from the LANCOM Systems homepage under www.lancom.eu/download/. We recommend that you update these programs before continuing to the installation.

1.1.5 Up-to-date firmware in the LANCOM

The latest firmware updates are available for download from the LANCOM Systems Web site under www.lancom.eu/download/. Select your device from the list and download the firmware onto your computer.

Detailed information about updating the firmware is available in the documentation for your LANCOM device.

1.2 Online registration

To activate the LANCOM Content-Filter Option in the LANCOM you need an activation code.

Please note: The activation code is not included in the package. It will be sent to you on online registration.

The LANCOM Content-Filter Option is supplied with a proof of license. This has a license number printed on it. This license number gives you one opportunity to register with LANCOM Systems and to receive an activation code.

After successful online registration, the license number of your LANCOM Content-Filter Option becomes invalid. The activation code that is sent to you can only be used with the LANCOM device as identified by the serial number which you provided at registration. Please ensure that you only want to install the LANCOM Content-Filter Option on the corresponding device. It is not possible to change to another device at a later date.

Necessary registration information

Please have the following information at the ready for your online registration:

- Precise designation of the software option

- The license number (from the proof of license)
- Serial number of your LANCOM (to be found on the underside of the device)
- Your customer data (company, name, postal address, e-mail address).

Registration is anonymous and can be completed without specifying personal data. Any additional information may be of help to us in case of service and support. All information is of course treated in the strictest confidence.

Online entry of registration information

① Start a web browser and access the LANCOM Systems web site under www.lancom.eu/routeroptions.

② Enter the information as required and follow the instructions that follow. After entering all of the data, you will be sent the activation code for your device and your customer data. If you submit an e-mail address you will receive the data including the activation code via e-mail. Online registration is now complete.

Make sure you store your activation code safely! You may need it at a later date to activate your LANCOM Content-Filter Option again, for example after a repair.

Help in case of problems

If you have problems with registering your software option, please contact us by e-mail at optionsupport@lancom.de.

1.3 Activating the LANCOM Content-Filter Option

Activating the LANCOM Content-Filter Option is very simple.

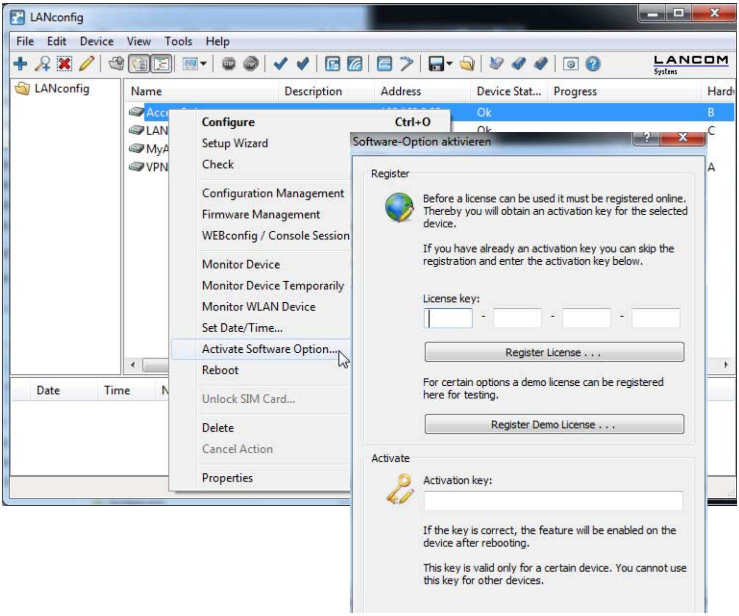
- In LANconfig, mark the appropriate device (simply click on the entry with your mouse) and select the menu item **Device** ▶ **Activate software option**. Alternatively, click on the entry for the device with the right-hand mouse key and select **Activate software option** from the context menu.
- Under WEBconfig you select the menu command **Extras** ▶ **Enable software option**.

  In the following window, enter the activation code that you received with your online registration. The device will then restart automatically.

- When using the command line interface (e.g. Telnet), enter the command **feature** followed by the activation key:

```
Feature <activation key>
```

Please be aware that activating the LANCOM Content-Filter Option is valid only for a certain time period. You can have an e-mail sent to you in good time before the license expires (WEBconfig: **LCOS menu tree ▶ Setup ▶ Config ▶ License expiry e-mail**).



Software-Option aktivieren

Register

Before a license can be used it must be registered online. Thereby you will obtain an activation key for the selected device.

If you have already an activation key you can skip the registration and enter the activation key below.

License key: ____ - ____ - ____ - ____

Register License . . .

For certain options a demo license can be registered here for testing.

Register Demo License . . .

Activate

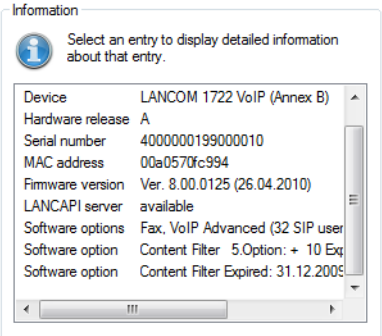
Activation key:

If the key is correct, the feature will be enabled on the device after rebooting.

This key is valid only for a certain device. You cannot use this key for other devices.

1.4 Checking the activation

You can check if the online activation of your LANCOM Content-Filter Option was successful by selecting the device in LANconfig and selecting the menu item **Device ▶ Properties**. The properties windows contains a tab named 'Info' that lists the activated software options.



Information

Select an entry to display detailed information about that entry.

Device	LANCOM 1722 VoIP (Annex B)
Hardware release	A
Serial number	4000000199000010
MAC address	00a0570fc994
Firmware version	Ver. 8.00.0125 (26.04.2010)
LANCAPI server	available
Software options	Fax, VoIP Advanced (32 SIP user
Software option	Content Filter 5.Option: + 10 Exp
Software option	Content Filter Expired: 31.12.2009

If activation was successful, you can continue by configuring the LANCOM Content-Filter.

2 Configuring the LANCOM Content Filter

2.1 Introduction

The LANCOM Content Filter enables you to filter certain content from your network, so preventing access to Internet pages with content that is illegal, dangerous or offensive. It also enables you to stop private surfing on specific sites during working hours. This not only increases staff productivity and network security but also ensures that the full bandwidth is available exclusively for your business activities.

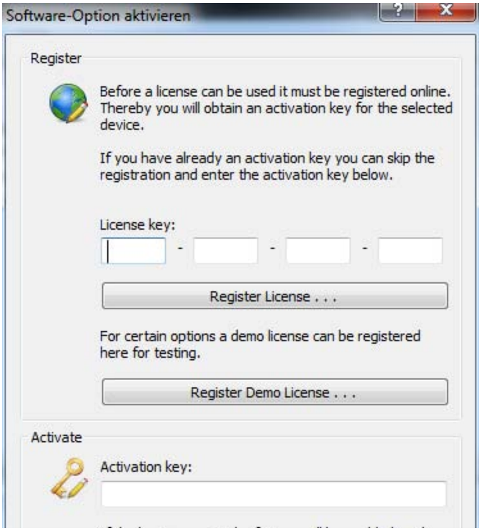
The LANCOM Content Filter is an intelligent content filter that works dynamically. It contacts a rating server that evaluates Internet sites reliably and accurately in accordance with the categories that you select.

The LANCOM Content Filter operates by checking the IP addresses behind the URLs that are entered. For any given domain it is possible to differentiate according to the path, meaning that specific areas of a URL may be rated differently.

It is not possible for users to avoid the LANCOM Content Filter website rating by entering the website's IP address into their browsers.
The LANCOM Content Filter checks only unencrypted websites via HTTP.

The LANCOM Content Filter license you purchase is valid for a certain number of users and for a specific period (for one or three years). You will be informed of the expiry of your license in good time. The number of current users is monitored in the device, with the users being identified by their IP address. You can configure what should happen when the number of licensed users is exceeded: Access can either be denied or an unchecked connection can be made.

You can test the LANCOM Content Filter on any router that supports this function. All you have to do is to activate a 30-day demo license for each device. Demo licenses are generated directly with LANconfig. Click on the device with the right-hand mouse key and select the context menu entry **Activate software option**. In the dialog that follows, click on the button **Demo license**. You will automatically be connected to the website for the LANCOM registration server. Simply select the required demo license and you can register your device.



Software-Option aktivieren

Register

Before a license can be used it must be registered online. Thereby you will obtain an activation key for the selected device.

If you have already an activation key you can skip the registration and enter the activation key below.

License key: | - | - | - |

For certain options a demo license can be registered here for testing.

Activate

Activation key:

All settings relating to categories are stored in category profiles. You select from predefined main and sub-categories in the LANCOM Content Filter: 58 categories are divided into 14 subject groups such as “Pornography, Nudity", "Shopping" or "Illegal Activities". You can activate or deactivate each of the categories in these groups. Sub-categories for “Pornography/Nudity” are, for example, “Pornography/Erotic/Sex” and “Swimwear/Lingerie”.

When configuring these categories, administrators have an additional option of activating an override. When the override option is active, users may still access the forbidden site for a particular period of time by clicking on a corresponding button, but the administrator will be notified of this by e-mail, syslog, or SNMP trap.

The category profile, whitelist and blacklist can be used to create a content filter profile that you can assign to particular users by means of the firewall. For example you can create a profile called “Employees_department_A” and assign this to all of the computers in that department.

When you install the LANCOM Content Filter, basic default settings are created automatically. These only need to be activated for the initial start. You can subsequently customize the behavior of the LANCOM Content Filter to match your own requirements.

2.2 Requirements for using the LANCOM Content Filter

The following requirements must be met before you can use the LANCOM Content Filter:

1. The firewall must be activated and an appropriate firewall rule must select the content filter profile.
2. The content filter profile must specify a category profile and if desired a whitelist and or blacklist for each part of the day. A content filter profile can consist of several different entries to provide different levels of protection during different parts of the day.

   If a certain part of the day is not covered by an entry, access to websites will go unchecked for this period.

ⓘ If the content filter profile is subsequently renamed, the firewall must also be modified.

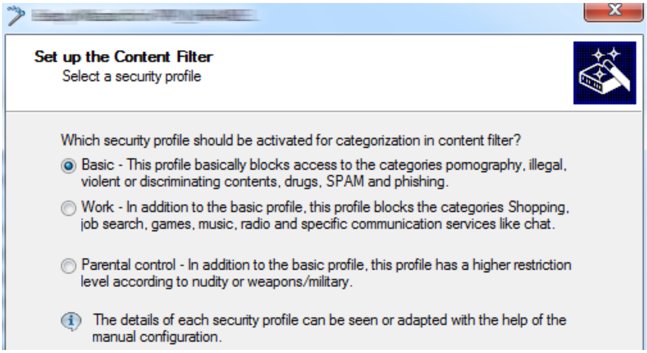
2.3 Quick start

After installing the LANCOM Content Filter, all the settings have been made to get it up and running quickly.

! The operation of the LANCOM Content Filter may be restricted by your country's data protection regulations or by company guidelines. Please check any regulations that may apply before putting the system into operation.

You activate the LANCOM Content Filter by:

1. Start the Setup Wizard for the device.
2. Select the Setup Wizard for configuring the Content Filter.



Set up the Content Filter

Select a security profile

Which security profile should be activated for categorization in content filter?

● Basic - This profile basically blocks access to the categories pornography, illegal, violent or discriminating contents, drugs, SPAM and phishing.

○ Work - In addition to the basic profile, this profile blocks the categories Shopping, job search, games, music, radio and specific communication services like chat.

○ Parental control - In addition to the basic profile, this profile has a higher restriction level according to nudity or weapons/military.

The details of each security profile can be seen or adapted with the help of the manual configuration.

3 Select one of the pre-defined security profiles (basic, work, parental control):

- □ Basic: This profile mainly blocks access to the categories pornography, illegal, violent or discriminatory content, drugs, SPAM and phishing
- □ Work: In addition to the settings for the basic profile, this profile also blocks the categories shopping, job search, gaming, music, radio and certain communications services such as chat.
- □ Parental-control: In addition to the settings for the basic profile, this profile also blocks nudity and weapons/military.

Should the firewall be deactivated, the Wizard will switch the firewall on. The Wizard then checks if the firewall rule is set correctly for the content filter and, if necessary, will take corrective measures. After activating the Content Filter with the steps outlined above, all stations in the network are being filtered according to the settings of the selected content-filter profile and the as-yet empty blacklist and whitelist. You can adapt these settings for your purposes, if necessary.

2.4 Default settings in LANCOM Content Filter

The following elements have been created in the default configuration of the LANCOM Content Filter:

- A firewall rule
- Three firewall action objects
- Three content filter profiles
- Two timeframes
- A blacklist

- A whitelist
- Three category profiles

Firewall rule

The preset firewall rule is named CONTENT-FILTER and uses the action object CONTENT-FILTER-BASIC.

The firewall rule is not created automatically if the LANCOM Content Filter is installed on a device that has been configured already. The rule must be added manually. This firewall rule must include one of the action objects that are pre-defined for the Content Filter.

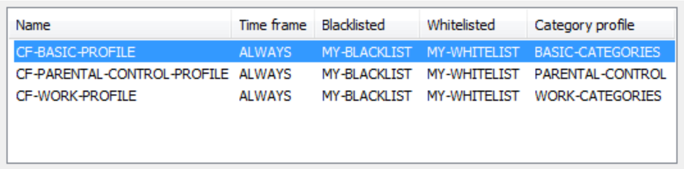
Firewall action objects

There are three firewall action objects: CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK and CONTENT-FILTER-PARENTAL-CONTROL. These action objects work with the corresponding content-filter profiles.

Content filter profiles

There are three content filter profiles. All content-filter profiles use the timeframe ALWAYS, the blacklist MY-BLACKLIST and the whitelist MY-WHITELIST. Each content-filter profile uses one of the predefined category profiles:

- CF-BASIC-PROFILE: This content-filter profile features a low level of restrictions and works with the category profile BASIC-CATEGORIES.
- CF-PARENTAL-CONTROL-PROFILE: This content-filter profile protects minors (e.g. trainees) from unsuitable Internet content, and it works with the category profile PARENTAL-CONTROL.
- CF-WORK-PROFILE: This content-filter profile is intended for companies wishing to place restrictions on categories such as Job Search or Chat. It works with the category profile WORK-CATEGORIES.



Name	Time frame	Blacklisted	Whitelisted	Category profile
CF-BASIC-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	BASIC-CATEGORIES
CF-PARENTAL-CONTROL-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	PARENTAL-CONTROL
CF-WORK-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	WORK-CATEGORIES

Timeframe

There are two predefined timeframes:

- ALWAYS: 00.00-23.59 hrs
- NEVER: 00.00-0.00 hrs

Blacklist

The preset blacklist is named "MY-BLACKLIST" and it is empty. Here you can optionally enter URLs which are to be forbidden.

Whitelist

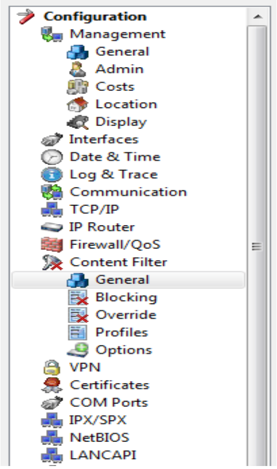
The preset whitelist is named "MY-WHITELIST" and it is empty. Here you can optionally enter URLs which are to be allowed.

Category profiles

There are three category profiles: BASIC-CATEGORIES, WORK-CATEGORIES and PARENTAL-CONTROL. The category profile specifies the categories which are to be allowed and forbidden, and for which one an override can be activated.

3 Advanced configuration of the LANCOM Content Filter with LANconfig

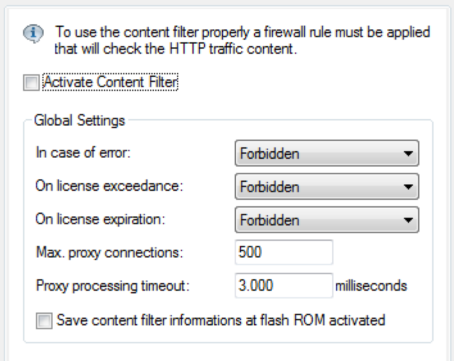
The program LANconfig contains a special menu to configure the content filter.



The operation of the LANCOM Content Filter may be restricted by your country's data protection regulations or by company guidelines. Please check any regulations that may apply before putting the system into operation.

3.1 General settings

Global settings for the LANCOM Content Filter are made here:



To use the content filter properly a firewall rule must be applied that will check the HTTP traffic content.

□ Activate Content Filter

Global Settings

In case of error: Forbidden

On license exceedance: Forbidden

On license expiration: Forbidden

Max. proxy connections: 500

Proxy processing timeout: 3.000 milliseconds

□ Save content filter informations at flash ROM activated

LANconfig: Content-Filter ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Global-Settings

- **Operating**

  This is where you can activate the LANCOM Content Filter.

- **Action-on-Error:**

  This is where you can determine what should happen when an error occurs. For example, if the rating server cannot be contacted, this settings either allows the user to surf without restrictions or access to the entire web is blocked.

  Possible values:

  □ Block, Pass

  Default:

  □ Block

- **Action-on-License-Exceedance:**

  This is where you can determine what should happen when the licensed number of users is exceeded. Users are identified by their IP address. The system keeps count of the IP addresses that connect via the LANCOM Content Filter. When the eleventh user establishes a connection with a 10-user license, no further checking is performed by the LANCOM Content Filter. Depending on this setting, the unlicensed user can either surf the web without restrictions, or access to the entire web is blocked.

  Possible values:

  □ Block, Pass

Default:

□ Block

The users of the content filter are automatically removed from the user list when no connection has been made from the IP address concerned via the content filter for 24 hours.

- **Action-on-License-Expiration:**

  The license to use the LANCOM Content Filter is valid for a certain period. You will be reminded of the license expiry date 30 days, one week and one day before it actually expires (at the e-mail address configured in LANconfig: Log & Trace ▶ General).

  This is where you can specify what should happen when the license expires (i.e. block everything or allow everything through). After the license used expires, this setting either allows the user to surf the web without restrictions, or access to the entire web is blocked.

  Possible values:

  □ Block, Pass

  Default:

  □ Block

- **Max. proxy connections**

  The maximum number of concurrent proxy connections can be configured here. The system load can be limited therewith. A notification is triggered if this limit will be exceeded. If the maximum number set here is exceeded, then the event defined for the proxy limit will be applied.

  Possible values:

  □ 0 to 999999 connections

  Default:

  □ device dependent

- **Proxy processing timeout**

  The time taken to check the URL can be limited. If the time set here is exceeded while the URL is being checked, then the event defined for errors will be applied.

  Possible values:

  □ Max. 9999 milliseconds

  Default:

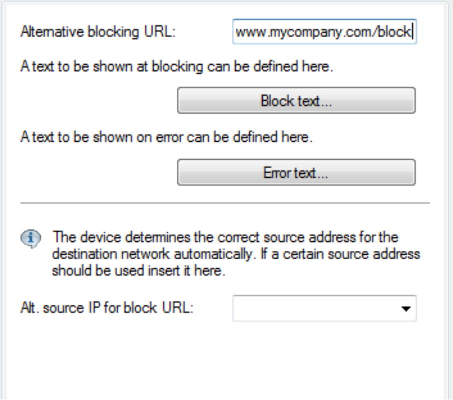
□ 3000 milliseconds

Special values:

□ The value 0 means unlimited timeout. Values smaller than 100 milliseconds are not reasonable.

3.2 Settings for blocking

You adjust the website-blocking settings here:



Alternative blocking URL: www.mycompany.com/block

A text to be shown at blocking can be defined here.

A text to be shown on error can be defined here.

The device determines the correct source address for the destination network automatically. If a certain source address should be used insert it here.

Alt. source IP for block URL:

LANconfig: Content-Filter ▶ Blocking

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Global-Settings

- **URL-To-Show-On-Blocking:**

  This is where you can enter the address of an alternative URL. If access is blocked, the URL entered here will be displayed instead of the requested website. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same HTML tags here as in blocking text. If you do not make any entry here, the default page stored in the device will be displayed..

  Possible values:

  □ Valid URL address

  Default:

  □ Blank

- **Alt. source IP for block URL:**

  This is where you can configure an optional sender address to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses you can specify them here as sender address.

  Possible values:

  □ Name of the IP networks whose address should be used

  □ "INT" for the address of the first intranet

  □ "DMZ" for the address of the first DMZ (caution: If there is an interface called "DMZ", its address will be taken in this case)

  □ LB0 ... LBF for the 16 loopback addresses

  □ GUEST

  □ Any IP address in the form x.x.x.x

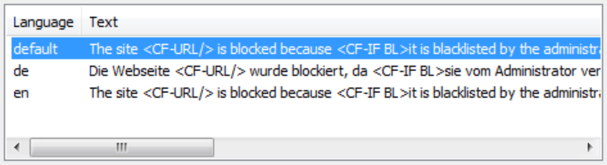
  Default:

  □ Blank

The sender address specified here is used unmasked for every remote station.

3.2.1 Block-Text

This is where you can define text to be displayed when blocking occurs. Different blocking texts can be defined for different languages. The display of blocking text is controlled by the language setting transmitted by the browser (user agent).



Language	Text
default	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr
de	Die Webseite <CF-URL/> wurde blockiert, da <CF-IF BL>sie vom Administrator ver
en	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr

- **Language**

  Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

  You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-USA

The country code must match the browser language setting exactly, e,g, "de-DE" must be entered for German ("de" on its own is not sufficient). If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

- 10 alphanumerical characters

Default:

- Blank

- **Text**

Enter the text that you wish to use as blocking text for this language.

Possible values:

- 254 alphanumerical characters

Default:

- Blank

Special values:

You can also use special tags for blocking text if you wish to display different pages depending on the reason why the website was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for a forbidden URL
- <CF-CATEGORIES/> for the list of categories why the website was blocked
- <CF-PROFILE/> for the profile name
- <CF-OVERRIDEURL/> for the URL used to activate the URL (this can be integrated in a simple <a> tag or in a button)

- <CF-LINK/> adds a link for activating the override
- <CF-BUTTON/> for a button for activating the override

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Possible attributes are:

- BLACKLIST: If the site was blocked because it is in the profile blacklist
- CATEGORY: If the site was blocked due to one of its categories
- ERR: If an error has occurred.

  Since there are separate text tables for the blocking page and the error page, this tag only makes sense if you have configured an alternative URL to show on blocking.
- OVERRIDEOK: If users have been allowed an override (in this case, the page should display an appropriate button)

If several attributes are defined in one tag, the section will be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

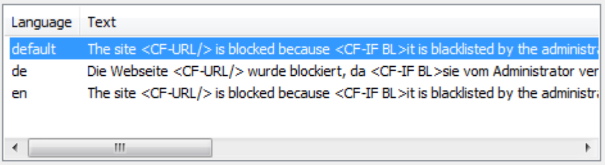
- Example:

  <CF-URL/> is blocked because it matches the categories <CF-CA/>.<br>Your content profile is <CF-PR/>.<br><CF-IF OVERRIDEOK><br><CF-BU/></CF-IF>

The tags described here can also be used in external HTML pages (alternative URLs to show on blocking).

3.2.2 Error-Text

This is where you can define text to be displayed when an error occurs.



Language	Text
default	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr
de	Die Webseite <CF-URL/> wurde blockiert, da <CF-IF BL>sie vom Administrator ver
en	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr

- **Language**

  This item offers the same settings as described under 'Language' →Page 18 above.

- **Text**

  Enter the text that you wish to use as error text for this language.

  Possible values:

  □ 254 alphanumerical characters

  Default:

  □ Blank

  Special values:

  You can also use HTML tags for the error text.

  The following empty element tags can be used as tag values:

  □ <CF-URL/> for a forbidden URL

  □ <CF-PROFILE/> for the profile name

  □ <CF-ERROR/> for the error message

  □ Example:

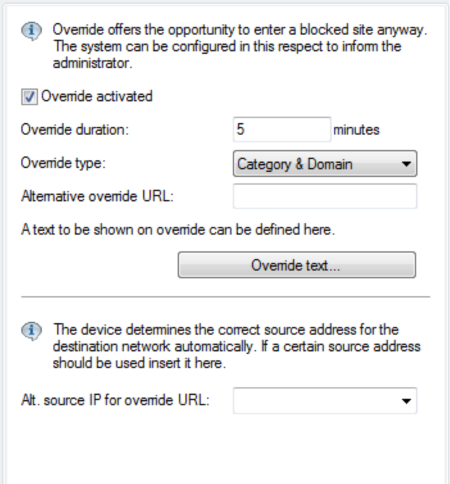
  <CF-URL/> is blocked because an error has occurred:<br><CF-ERROR/>

3.3 Override settings

The override function allows a website to be accessed even though it is classified as forbidden. The user must click on the override button to confirm that the forbidden page should be opened. You can configure this feature so that the administrator is notified when the override button is clicked (LANconfig: Content-Filter ▶ Global-Settings).

> ! If the override type "Category" has been activated, clicking on the override button makes **all** of the categories for that URL accessible to the user The next blocking page to be displayed has just one category explaining why access to the URL was blocked. After clicking on the override button, all of the allowed categories are displayed. If the override type "Domain" has been activated, then the entire domain can be accessed.

The settings for the override function are to be found here:



Override offers the opportunity to enter a blocked site anyway. The system can be configured in this respect to inform the administrator.

☑ Override activated

Override duration: 5 minutes

Override type: Category & Domain

Alternative override URL:

A text to be shown on override can be defined here.

The device determines the correct source address for the destination network automatically. If a certain source address should be used insert it here.

Alt. source IP for override URL:

LANconfig: Content-Filter ▶ Override

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Global-Settings

- **Override-Active**

  This is where you can activate the override function and make further related settings.

- **Override-Duration**

  The override duration can be restricted here. When the period expires, any attempt to access the same domain and/or category will be blocked again. Clicking on the override button once more allows the website to be accessed again for the duration of the override and, depending on the settings, the administrator will be notified once more.

  Possible values:

  □ 1-1440 (minutes)

  Default:

  □ 5 (minutes)

- **Override-Type:**

  This is where you can set the type of override. It can be allowed for the domain, for the category of website to be blocked, or for both.

  Possible values:

- □ Category: For the duration of the override, all URLs are allowed that fall under the affected categories (as well as those which would already have been allowed even without the override).
- □ Domain: For the duration of the override all URLs in this domain are allowed, irrespective of the categories they belong to.
- □ Category-and-Domain: For the duration of the override, all URLs are allowed that belong to this domain and also to the allowed categories. This is the highest restriction.

Default:

- □ Category-and-Domain

- **URL-To-Show-On-Override:**

  This is where you can enter the address of an alternative URL. In the event of an override, the URL entered here will be displayed instead of the usual website. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as in the override text. If you do not make any entry here, the default page stored in the device will be displayed..

  Possible values:

  - □ Valid URL address

  Default:

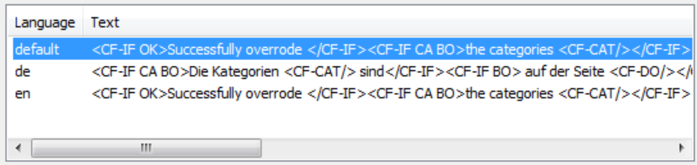
  - □ Blank

- **Override sender IP address:**

  This item offers the same settings as under ’Alt. source IP for block URL:’ →Page 18.

3.3.1 Override text

This is where you can define text that is displayed to users confirming an override.



Language	Text
default	<CF-IF OK>Successfully overrode </CF-IF><CF-IF CA BO>the categories <CF-CAT/></CF-IF>
de	<CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> auf der Seite <CF-DO/></
en	<CF-IF OK>Successfully overrode </CF-IF><CF-IF CA BO>the categories <CF-CAT/></CF-IF>

- **Language**

  This item offers the same settings as described under 'Language' →Page 18 above.

- **Text**

  Enter the text that you wish to use as override text for this language.

  Possible values:

  □ 254 alphanumerical characters

  Default:

  □ Blank

  Special values:

  You can also use HTML tags for blocking text if you wish to display different pages depending on the reason why the website was blocked (e.g. forbidden category or entry in the blacklist).

  The following tags can be used as tag values:

  □ <CF-URL/> for the originally forbidden URL that is now allowed

  □ <CF-CATEGORIES/> for the list of categories that have now been allowed as a result of the override (except if domain override is specified).

  □ <CF-BUTTON/> displays an override button that forwards the browser to the original URL.

  □ <CF-BUTTON/> displays an override link that forwards the browser to the original URL.

  □ <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.

  □ <CF-ERROR/> generates an error message in the event that the override fails.

  □ <CF-DURATION/> displays the override duration in minutes.

  You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

  Attributes can be:

  □ CATEGORY when the override type is "Category" and the override was successful

  □ DOMAIN when the override type is "Domain" and the override was successful

- □ BOTH when the override type is "Category-and-Domain" and the override was successful
- □ ERROR when the override fails
- □ OK if either CATEGORY or DOMAIN or BOTH are applicable

If several attributes are defined in one tag, the section should be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

- □ Example:

  <CF-IF CA BO>Categories <CF-CAT/> are </CF-IF><CF-IF BO> in domain <CF-DO/></CF-IF><CF-IF DO>. Access to domain <CF-DO/> is allowed for </CF-IF><CF-IF OK> f&uuml;r <CF-DU/> minutes. <br><CF-LI/></CF-IF><CF-IF ERR>Override error :<br><CF-ERR/ ></CF-IF>

3.4 Profiles in the LANCOM Content Filter

This is where you can create content filter profiles that are used to check websites for prohibited content. A content filter profile always has a name and, for various time periods, it activates the desired category profile and, optionally, a blacklist and a whitelist.

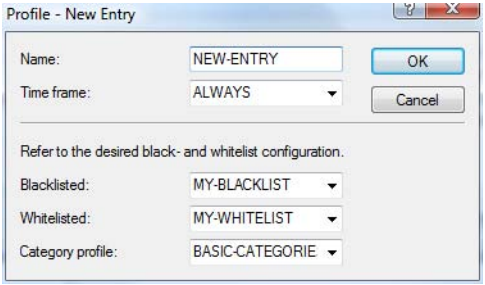
In order to provide different configurations for the various timeframes, several content-filter profile entries are created with the same name. The content filter profile is thus made up of the sum of all entries with the same name.

The firewall refers to this content-filter profile.

Please note that you must make corresponding settings in the firewall in order to use the profiles in the LANCOM Content Filter.

3.4.1 Profiles

The settings for the profiles are to be found here:



Name: NEW-ENTRY

Time frame: ALWAYS

Refer to the desired black- and whitelist configuration.

Blacklisted: MY-BLACKLIST

Whitelisted: MY-WHITELIST

Category profile: BASIC-CATEGORIE

LANconfig: Content-Filter ▶ Profiles ▶Profiles

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profiles ▶ Profiles

- **Name**

  The profile name that the firewall references must be specified here.

  Possible values:

  □ Name of a profile

  Default:

  □ Blank

- **Timeframe**

  Select the timeframe for this category profile and, optionally, the blacklist and the whitelist. The timeframes “ALWAYS” and “NEVER” are predefined. You can configure other timeframes under:

  LANconfig: Date/Time ▶ General ▶ Timeframe

  WEBconfig: LCOS menu tree ▶ Setup ▶ Time ▶ Timeframe

  One profile may have several lines with different timeframes.

  Possible values:

  □ Always
  □ Never
  □ Name of a timeframe profile

  Default:

  □ Blank

If timeframes overlap when multiple entries are used for a content filter profile, all pages contained in one of the active entries will be blocked for that period of time. If a period remains undefined when several entries are used for a content filter profile, access to all websites is unchecked for this period.

- **Blacklist**

  Name of the blacklist profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the blacklist table.

  Possible values:

  □ Name of a blacklist profile

  □ New name

  Default:

  □ Blank

- **Whitelist**

  Name of the whitelist profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the whitelist table.

  Possible values:

  □ Name of a whitelist profile

  □ New name

  Default:

  □ Blank

- **Category-Profile**

  Name of the category profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the category table.

  Possible values:

  □ Name of a category profile

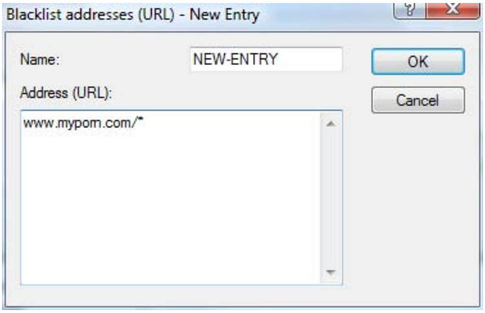
  □ New name

  Default:

  □ Blank

3.4.2 Blacklist addresses (URL)

This is where you can configure websites which are to be blocked.



Blacklist addresses (URL) - New Entry

Name: NEW-ENTRY

Address (URL):

www.mypom.com/*

LANconfig: Content-Filter ▶ Profiles ▶Blacklist addresses (URL)

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profiles ▶ Blacklists

- **Name**

  Enter the name of the blacklist for referencing from the content-filter profile.

  Possible values:

  □ Blacklist name

  Default:

  □ Blank

- **Address (URL)**

  Access to the URLs entered here will be forbidden by the blacklist.

  Possible values:

  □ Valid URL address

  The following wildcard characters may be used:

  □ * for any combination of more than one character (e.g. www.lancom.* encompasses the websites www.lancom.de, www.lancom.eu, www.lancom.es, etc.)

  □ ? * for any one character (e.g. www.lancom.e* encompasses the websites www.lancom.eu, www.lancom.es)

Please enter the URL **without** the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/ . For this reason it is advisable to enter the URL as: www.mycompany.de* .

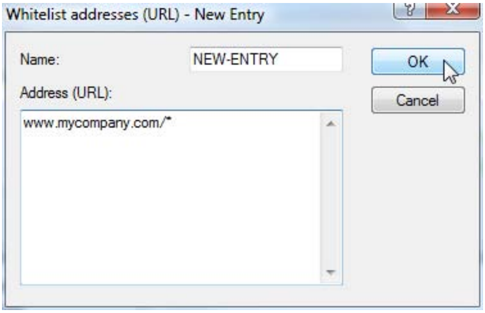
Individual URLs are separated by a blank.

Default:

□ Blank

3.4.3 Whitelist addresses (URL)

This is where you can configure websites to which access is to be allowed.



Whitelist addresses (URL) - New Entry

Name: NEW-ENTRY

Address (URL): www.mycompany.com/*

LANconfig: Content-Filter ▶ Profiles ▶Whitelist addresses (URL)

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profiles ▶ Whitelists

- **Name**

  Enter the name of the whitelist for referencing from the content-filter profile.

  Possible values:

  □ Name of a whitelist

  Default:

  □ Blank

- **Addresses (URL)**

  This is where you can configure websites which are to be checked locally and then accepted.

  Possible values:

  □ Valid URL address

  The following wildcard characters may be used:

- * for any combination of more than one character (e.g. www.lancom.* encompasses the websites www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? * for any one character (e.g. www.lancom.e* encompasses the websites www.lancom.eu, www.lancom.es)

Please enter the URL **without** the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/ . For this reason it is advisable to enter the URL as: www.mycompany.de* .

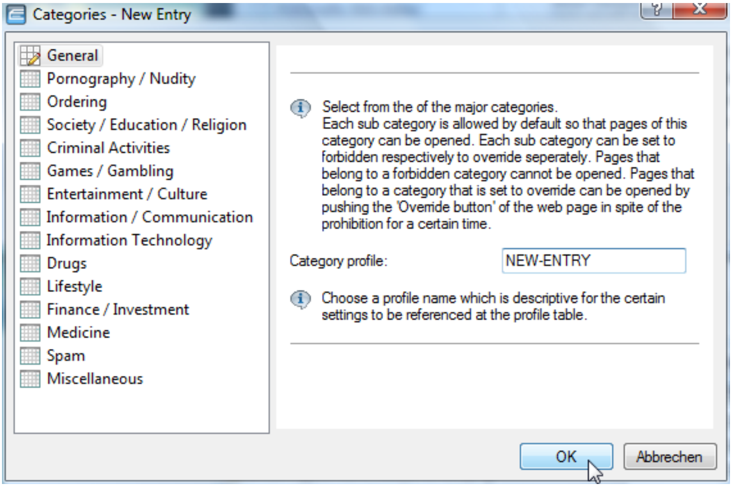
Individual URLs are separated by a blank.

Default:

- Blank

3.4.4 Category-Profiles

Here you create a category profile and determine which categories or groups should be used to rate websites for each category profile. You can allow or forbid the individual categories or activate the override function for each group.



Select from the of the major categories.
Each sub category is allowed by default so that pages of this category can be opened. Each sub category can be set to forbidden respectively to override seperately. Pages that belong to a forbidden category cannot be opened. Pages that belong to a category that is set to override can be opened by pushing the 'Override button' of the web page in spite of the prohibition for a certain time.

Category profile: NEW-ENTRY

Choose a profile name which is descriptive for the certain settings to be referenced at the profile table.

LANconfig: Content-Filter ▶ Profiles ▶Categories

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profiles ▶ Category-Profiles

- **Category profile**

  The name of the category profile for referencing from the content-filter profile is entered here.

  Possible values:

  □ Name of a category profile

  Default:

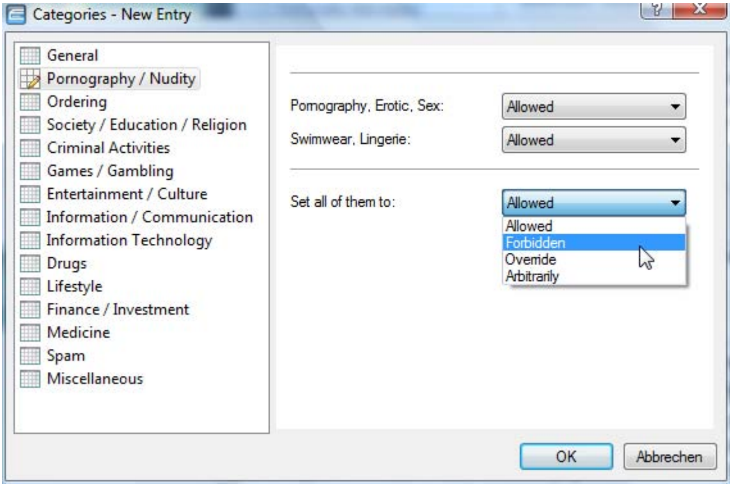
  □ Blank

- **Category settings**

  For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

  The following main categories can be configured:

  □ Pornography/Nudity
  □ Shopping
  □ Society/Education/Religion
  □ Illegal Activities
  □ Games/Gaming
  □ Entertainment/Culture
  □ Information/Communication
  □ Information Technology
  □ Drugs
  □ Lifestyle
  □ Finance/Investment
  □ Medicine
  □ Spam
  □ Miscellaneous



Pornography, Erotic, Sex: Allowed

Swimwear, Lingerie: Allowed

Set all of them to: Allowed

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

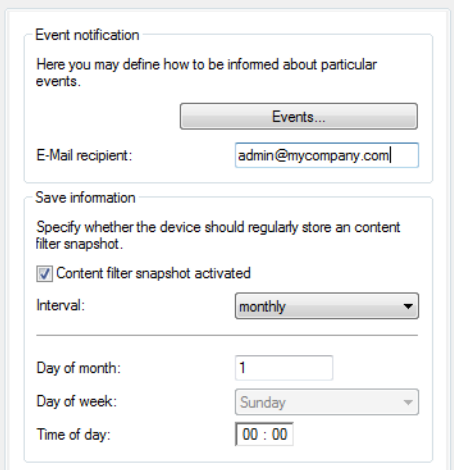
- Allowed, forbidden, override

Default:

- Allowed

3.5 Options with the LANCOM Content Filter

This is where you can determine whether you wish to be notified of events and where LANCOM Content Filter information is to be stored.



Event notification

Here you may define how to be informed about particular events.

E-Mail recipient: admin@mycompany.com

Save information

Specify whether the device should regularly store an content filter snapshot.

☑ Content filter snapshot activated

Interval: monthly

Day of month: 1

Day of week: Sunday

Time of day: 00 : 00

LANconfig: Content-Filter ▶ Options

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Global-Settings

- **Events:**

  This is where you define how you wish to receive notification of specific events. Notification can be made by e-mail, SNMP or SYSLOG. You can specify that messages for different events should be output in different ways.

  Error:

  - For SYSLOG: Source “System”, priority “Alarm”.
  - Default: SNMP notification

  License expiration:

  - For SYSLOG: Source “Admin”, priority “Alarm”.
  - Default: SNMP notification

  License exceeded:

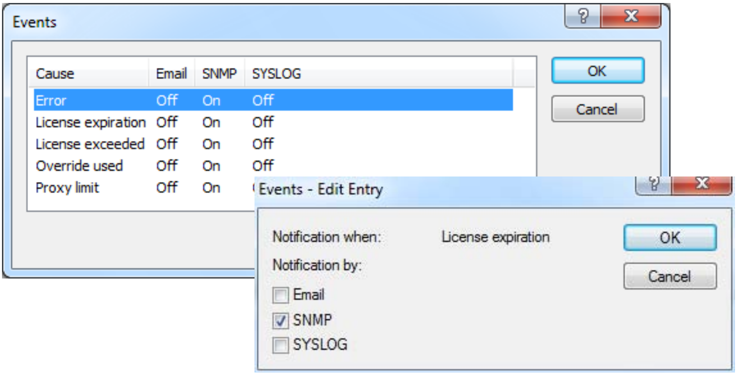
  - For SYSLOG: Source “Admin”, priority “Alarm”.
  - Default: SNMP notification

  Override applied:

  - For SYSLOG: Source “Router”, priority “Alarm”.
  - Default: SNMP notification

  Proxy Limit:

- □ For SYSLOG: Source “Admin”, priority “Info”.
- □ Default: SNMP notification



Events

Cause	Email	SNMP	SYSLOG
Error	Off	On	Off
License expiration	Off	On	Off
License exceeded	Off	On	Off
Override used	Off	On	Off
Proxy limit	Off	On	

Events - Edit Entry

Notification when: License expiration

Notification by:

☐ Email

☑ SNMP

☐ SYSLOG

- ■ **E-mail recipient:**

  An SMTP client must be defined if you wish to use the e-mail notification function. You can use the client in the device, or another client of your choice.

No e-mail will be sent if no e-mail recipient is defined,.

- ■ **Content-Filter-Snapshot**

  This is where you can activate the content filter snapshot and determine when and how often it should be taken. The snapshot copies the category statistics table to the last snapshot table, overwriting the old contents of the snapshot table. The category statistics values are then reset to 0.

- ■ **Interval**

  Here you decide whether the snapshot should be taken monthly, weekly or daily.

  Possible values:

  - □ Monthly
  - □ Weekly
  - □ Daily

  Default:

  - □ Monthly

- **Day of month:**

  For monthly snapshots, set the day of the month when the snapshot should be taken.

  Possible values:

  □ Max. 2 characters

  Default:

  □ 1

ⓘ It is advisable to select a number between 1 and 28 in order to ensure that it occurs every month.

- **Weekday:**

  For weekly snapshots, set the day of the week when the snapshot should be taken.

  Possible values:

  □ Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

  Default:

  □ Monday

- **Time:**

  If you require a daily snapshot, then enter here the time of day for the snapshot in hours and minutes.

  Possible values:

  □ Maximum 5 characters, format HH:MM

  Default:

  □ 00:00

3.6 Additional settings for the LANCOM Content Filter

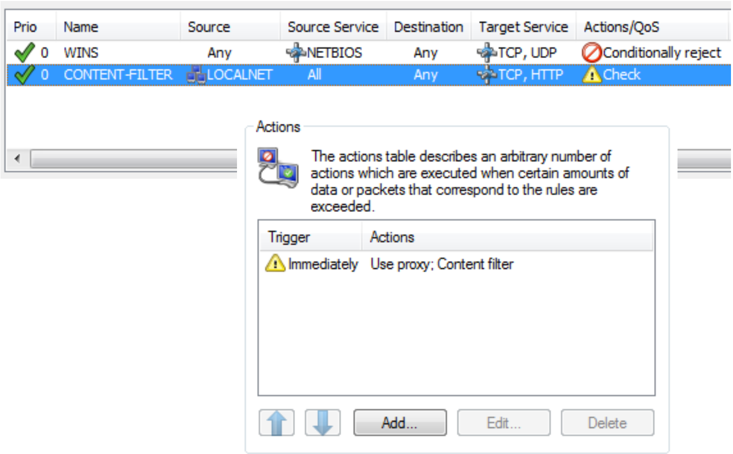
3.6.1 Firewall settings for the content filter

The firewall must be activated in order for the LANCOM Content Filter to function. You can activate the firewall under:

LANconfig: Firewall/QoS ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-Router ▶ Firewall

In the default configuration, you will find the firewall rule CONTENT-FILTER that refers to the action object CONTENT-FILTER-BASIC:



Prio	Name	Source	Source Service	Destination	Target Service	Actions/QoS
✓ 0	WINS	Any	NETBIOS	Any	TCP, UDP	Conditionally reject
✓ 0	CONTENT-FILTER	LOCALNET	All	Any	TCP, HTTP	Check

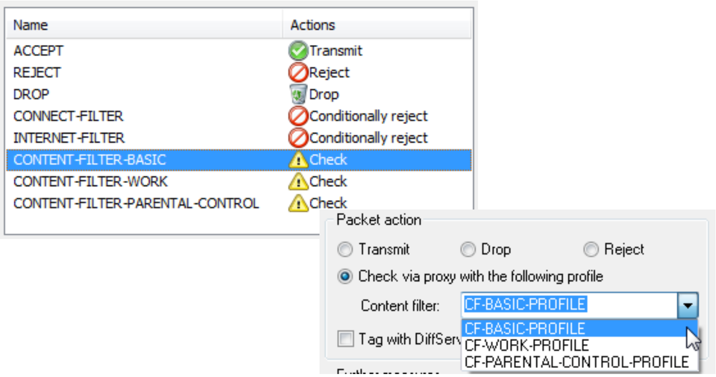
Actions

The actions table describes an arbitrary number of actions which are executed when certain amounts of data or packets that correspond to the rules are exceeded.

Trigger	Actions
Immediately	Use proxy; Content filter

The firewall rule should be limited to the target service “http” so that only outgoing HTTP connections are examined. Without this restriction all packets will be checked by the content filter, which could lead to a loss of system performance.

A content-filter related firewall rule must contain a special action object that uses packet actions to check the data according to a content-filter profile. In the default configuration you will find the action objects CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK and CONTENT-FILTER-PARENTAL-CONTROL, each of which refer to their corresponding content-filter profile:



Name	Actions
ACCEPT	Transmit
REJECT	Reject
DROP	Drop
CONNECT-FILTER	Conditionally reject
INTERNET-FILTER	Conditionally reject
CONTENT-FILTER-BASIC	Check
CONTENT-FILTER-WORK	Check
CONTENT-FILTER-PARENTAL-CONTROL	Check

Packet action

○ Transmit ○ Drop ○ Reject

● Check via proxy with the following profile

Content filter: CF-BASIC-PROFILE

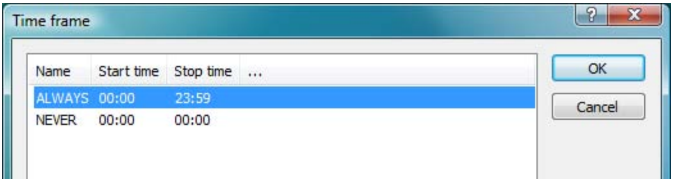
□ Tag with DiffSer

Example: When a web page is accessed, the data packets pass through the firewall and are processed by the rule CONTENT-FILTER. The action object CONTENT-FILTER-BASIC checks the data packets using the content-filter profile CONTENT-FILTER-BASIC.

3.6.2 Timeframe

Timeframes are used to define the periods when the content-filter profiles are valid. One profile may have several lines with different timeframes. Different lines in a timeframe should complement each other, i.e. if you specify WORKTIME you will probably wish to specify a timeframe called FREETIME to cover the time outside of working hours.

The timeframes "ALWAYS" and "NEVER" are predefined. You can configure other timeframes under:



Name	Start time	Stop time	...
ALWAYS	00:00	23:59	
NEVER	00:00	00:00	

LANconfig: Date/Time ▶ General ▶ Timeframe

WEBconfig: LCOS menu tree ▶ Setup ▶ Time ▶ Timeframe

- **Name**

  Enter the name of the timeframe for referencing from the content-filter profile.

  Possible values:

  □ Name of a timeframe

  Default:

  □ Blank

- **Start**

  Here you set the start time (time of day) when the selected profile becomes valid.

  Possible values:

  □ Maximum 5 characters, format HH:MM

  Default:

  □ 00:00

- **Stop time**

  Here you set the stop time (time of day) when the selected profile ceases to be valid.

  Possible values:

  □ Maximum 5 characters, format HH:MM

  Default:

  □ 23:59

- **Weekdays**

  Here you select the weekday on which the timeframe is to be valid.

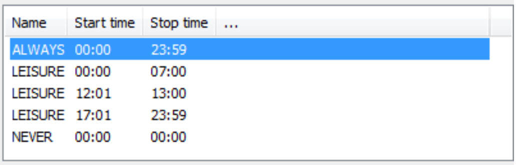
  Possible values:

  □ Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

  Default:

  □ Activated for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

  You can form a time schedule with the same name but with different times extending over several lines:

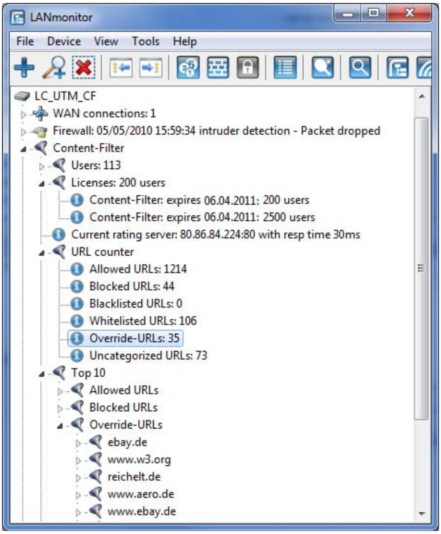


Name	Start time	Stop time	...
ALWAYS	00:00	23:59	
LEISURE	00:00	07:00	
LEISURE	12:01	13:00	
LEISURE	17:01	23:59	
NEVER	00:00	00:00	

4 Status messages

4.1 LANmonitor

LANmonitor allows you to see the most important status messages from the LANCOM Content Filter at a glance.



```
LC_UTM_CF
  WAN connections: 1
  Firewall: 05/05/2010 15:59:34 intruder detection - Packet dropped
  Content-Filter
    Users: 113
    Licenses: 200 users
      Content-Filter: expires 06.04.2011: 200 users
      Content-Filter: expires 06.04.2011: 2500 users
    Current rating server: 80.86.84.224:80 with resp time 30ms
    URL counter
      Allowed URLs: 1214
      Blocked URLs: 44
      Blacklisted URLs: 0
      Whitelisted URLs: 106
      Override-URLs: 35
      Uncategorized URLs: 73
    Top 10
      Allowed URLs
      Blocked URLs
      Override-URLs
        ebay.de
        www.w3.org
        reichelt.de
        www.aero.de
        www.ebay.de
```

4.1.1 Information displayed by LANCOM Content Filter in summary

LANmonitor shows the the following information about the LANCOM Content Filter:

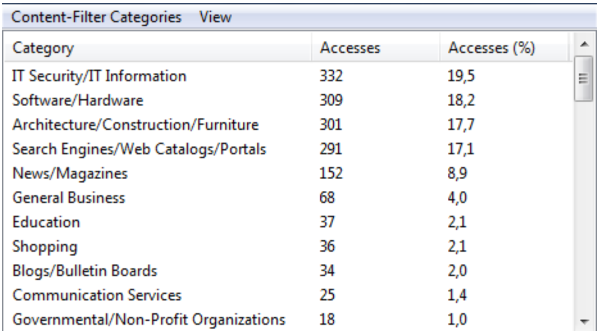
- IP addresses and MAC addresses of the users
- LANCOM Content Filter license information
- Information on the currently used content-filter server
  - Used since: The time when the specified rating server was first used.
  - First response time: Time taken for the rating server to respond the first time.
  - URLs processed: Number of processed URLs.
  - Processing timeouts: Number of times that URL processing exceeded the timeout period.
  - Minimum processing time: Minimum time taken to process a URL.

  - Maximum processing time: Maximum time taken to process a URL, assuming this is less than the timeout value.
  - Average processing time: Average time taken to process a URL.
  - Average processing time (last 5 min.): The average time taken to process a URL in the last 5 minutes.
  - Requests to rating server: Number of URL requests processed by the rating server.
  - Rating server timeouts: Number of times that URL processing by the rating server exceeded the timeout period.
  - Minimum rating server response time: Minimum time taken for the rating server to process a request.
  - Maximum rating server response time: Maximum time taken for the rating server to process a request, assuming this is less than the timeout value.
  - Average rating server response time: Average time taken for the rating server to process a request.
  - Average rating server response time (last 5 min.): Average time taken for the rating server to process requests in the last 5 minutes.
- URL counter showing allowed URLs, blocked URLs, blacklisted and whitelisted URLs, override URLs and uncategorized URLs. (Only URLs without paths are counted).
- URL counter for blocked URLs, blacklisted URLs, whitelisted URLs, URLs accessed by override, uncategorized URLs.
- Top 10 allowed URLs, blocked URLs and URLs accessed using the override function. The category determined and the number of accesses are displayed.
- Cache use: Cache usage for categorizing URLs.
- Cache hit rate: Proportion of URL requests that were answered by the cache memory.

4.1.2 Detailed displays in LANCOM Content Filter

You can open two additional windows via the LANCOM Content Filter menu. Simply click on the entry "Content-Filter" with the right-hand mouse key and select the corresponding entry from the context menu.

Displaying content filter category statistics

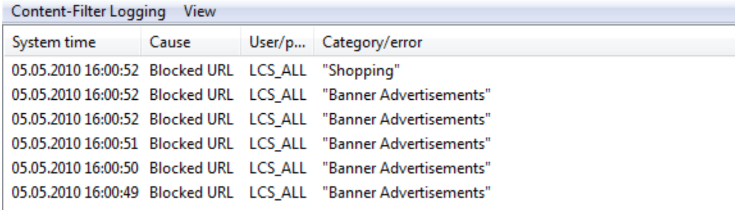


Category	Accesses	Accesses (%)
IT Security/IT Information	332	19,5
Software/Hardware	309	18,2
Architecture/Construction/Furniture	301	17,7
Search Engines/Web Catalogs/Portals	291	17,1
News/Magazines	152	8,9
General Business	68	4,0
Education	37	2,1
Shopping	36	2,1
Blogs/Bulletin Boards	34	2,0
Communication Services	25	1,4
Governmental/Non-Profit Organizations	18	1,0

This dialog displays the list of all categories with the number of blocked accesses to the content filter and the share of all accesses in percent.

You can use the **Content-Filter categories** menu to save the currently displayed values to a file or to load saved values for display in the LANmonitor.

Displaying the Content-Filter Log



System time	Cause	User/p...	Category/error
05.05.2010 16:00:52	Blocked URL	LCS_ALL	"Shopping"
05.05.2010 16:00:52	Blocked URL	LCS_ALL	"Banner Advertisements"
05.05.2010 16:00:52	Blocked URL	LCS_ALL	"Banner Advertisements"
05.05.2010 16:00:51	Blocked URL	LCS_ALL	"Banner Advertisements"
05.05.2010 16:00:50	Blocked URL	LCS_ALL	"Banner Advertisements"
05.05.2010 16:00:49	Blocked URL	LCS_ALL	"Banner Advertisements"

This dialog displays the logged information for each individual access to the content filter with the following details:

- System time
- Cause of the log entry
- User/profile
- Category/Error
- URL called

You can reset (flush) the currently displayed values in the **Content-Filter Log** menu.

4.1.3 Functions in LANmonitor

Additional functions are available for you to influence the LANmonitor display:

- Click with the right-hand mouse button on the URL counter entry in LANmonitor and select **Reset URL counter** to reset the values for this particular area to zero.
- Click on the right-hand mouse button on the Top-10 entry in LANmonitor and select**Flush Top-10 lists and cache** to reset the values for this particular area to zero.

4.2 WEBconfig

Besides the status information displayed in LANmonitor you can access all status messages with WEBconfig under:

WEBconfig: LCOS menu tree ▶ Status ▶UTM ▶Content-Filter

The individual status messages are described below:

- **Uncategorized-URLs**

  Displays the number of websites accessed that are not assigned to a category.
- **Blacklisted-URLs**

  Displays the number of websites accessed that are on the blacklist.
- **Allowed-URLs**

  Number of websites that were accessed and which were allowed.
- **Error-Count**

  Displays the number of errors. An error can occur for example when the rating server cannot be contacted.
- **Blocked-URLs**

  Number of websites that were called and which were blocked.
- **License-Count**

  Number of licenses you have purchased. You can purchase additional licenses from your distributor.
- **Overridden-URLs**

  Number of websites accessed using the override function. You can set the override function to allow users to open a website following a prompt indicating that it is forbidden.

- **Whitelisted-URLs**

  Displays the number of websites accessed that are on the whitelist.
- **Cache-Flush**

  This option allows you to delete (flush) the cache and all Top-10 lists. The Cache-Current-Size is reset to 0 while the Cache-Maximum-Size remains unchanged.
- **Category-Statistics-Flush**

  This option allows you to delete (flush) the category statistics and the last snapshot.
- **Log-Flush**

  This option allows you to delete (flush) the log table and the override log.
- **Statistics-Flush**

  This option allows you to delete (flush) the statistics. The counters are reset to 0.

4.2.1 Users

The user table displays the IP address and the MAC address of all current users of the content filter.

- **IP address**

  Displays the user's IP address.
- **MAC address**

  Displays the user's MAC address.

4.2.2 Category statistics

The category statistics show all the categories and the number of websites assigned to these categories that have been called by a user.

- **Category**

  Name of the category in question.
- **Hits**

  Number of websites called that are assigned to the relevant category.

4.2.3 Last-Snapshot

The list of the last snapshot displays all categories and the number of websites assigned to these categories that have been called by a user. You can configure how often a snapshot is taken (see ’Options with the LANCOM

Content Filter' →Page 32). The snapshot copies the category statistics table to the last last snapshot table, overwriting the contents of the last snapshot table. The category statistics values are then reset to 0.

- **Category**

  Name of the category in question.

- **Hits**

  Number of websites called that are assigned to the relevant category.

4.2.4 Log

The log table displays the system time of the log, the cause for the log and additional information on the user profile, category or error and the URL.

- **System-time**

  Indicates the time of the log.

- **Cause**

  Indicates the cause of the log.

- **User/profile**

  The name of the user profile or the IP address of the user.

- **Category/Error**

  If the site was forbidden, the list of categories or the name of the blacklist that caused the website to be blocked is displayed here.

  If the site could not be displayed due to an error, the cause of the error is indicated.

  When the number of licenses is exceeded, this entry indicates whether the site was blocked or allowed.

- **URL**

  The URL that the user wishes to access.

  If the number of licenses is exceeded or if the license has expired, this entry remains empty.

4.2.5 Override-Log

- **Date/Time**

  Indicates the date and time of the override.

- **User-IP**

  Indicates the IP address of the user who performed the override.

- **User-MAC**

  Indicates the MAC address of the user who performed the override.
- **Target URL**

  Indicates the website for which the override was performed.

4.2.6 Cache

- **Cache-Current-Size**

  Indicates the current size of the cache. The cache stores the categorizations for the URLs that the evaluation server queries. There is one cache entry for each domain. The cache size influences how often the server needs to be queried.
- **Cache-Maximum-Size**

  This displays the maximum size of the cache. The cache stores the categorizations for the URLs that the evaluation server queries. There is one cache entry for each domain. The cache size influences how often the server needs to be queried.
- **Hit ratio in %**

  Proportion of URL requests that were answered by the cache memory.

Top-10-Allowed Hosts

This table lists the ten most frequently accessed websites from the whitelist.

- **Host**

  Indicates the host of the website.
- **Category**

  Indicates the category that the website is assigned to.
- **Hits**

  Number of allowed calls of this website.

Top-10-Blocked Hosts

This table lists the ten most frequent websites from the blacklist for which access attempts are made.

- **Host**

  Indicates the host of the website.
- **Category**

  Indicates the category that the website is assigned to.

- **Hits**

  Number of attempted calls of this website.

Top-10-Overidden-Hosts

This table lists the ten most frequently called websites accessed using the override function.

- **Host**

  Indicates the host of the website.

- **Category**

  Indicates the category that the website is assigned to.

- **Hits**

  Number of calls of this website that were allowed on the basis of an active override.

4.2.7 Performance

- **5min proc time**

  The average time taken to process a URL in the last 5 minutes.

- **5min serv time**

  Average time taken for the rating server to process requests in the last 5 minutes.

- **Ini serv time**

  Time taken for the rating server to respond the first time.

- **Used since**

  The time when the specified rating server was first used.

- **Proc URLs**

  Number of processed URLs.

- **Max proc time**

  Maximum time taken to process a URL, assuming this is less than the timeout value.

- **Max serv time**

  Maximum time taken for the rating server to process a request, assuming this is less than the timeout value.

- **Min proc time**

  Minimum time taken to process a URL.

- **Min serv time**

  Minimum time taken for the rating server to process a request.

- **Avg proc time**

  Average time taken to process a URL.

- **Avg serv time**

  Average time taken for the rating server to process a request.

- **Proc timeouts**

  Number of times that URL processing exceeded the timeout period.

- **Rating server**

  Indicates the current server that the content filter contacts and that rates the websites reliably and accurately in accordance with the categories you select.

- **Serv requests**

  Number of URL requests processed by the rating server.

- **Server timeouts**

  Number of times that URL processing by the rating server exceeded the timeout period.

Performance log

This table lists the above values for each rating server used. You can check the history of the rating server's performance.

4.2.8 Proxy connections

This menu contains information on the statistical values about the content filter's use of proxies.

- **Denied connection attempts**

  Number of connections not accepted by the content-filter proxy.

- **Current connections**

  Current number of active connections to the content-filter proxy.

- **Avg connections**

  The average number of connections to the content-filter proxy.

- **Total connections**

  The total number of connections to the content-filter proxy.

- **Max connections**

  The maximum number of simultaneous connections to the content-filter proxy.
- **Proxy connections limit**

  The maximum allowed number of connections to the content-filter proxy.
- **5min avg connections**

  Number of connections to the content-filter proxy in the last 5 minutes.
- **Connection statistics since**

  The time when collection of the connection statistics started.

5 Tutorial: Using multiple content filter profiles

This chapter shows how to use a number of content filter profiles to good effect and the settings that should be considered.

The LANCOM Content Filter allows you to configure several content filter profiles. You can use this option in order to create, for example, one content filter profile for your employees and another content filter profiles for trainees. When a company employs trainees under the age of eighteen this may not only be useful but also a legal requirement.

The following example describes the steps you should take to set up various content filter profiles for your employees and your trainees.

1. Activate the LANCOM Content Filter:

   LANconfig: Content-Filter ▶ General

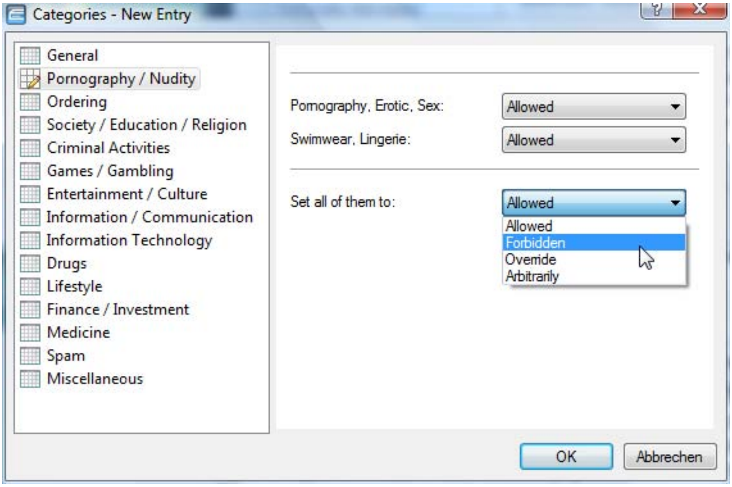
   WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Operating Yes

2. Create a content filter profile under:

   LANconfig: Content-Filter ▶ Profiles

   WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profiles ▶ Profiles

3. Create one or more category profiles under **Category-Profiles** and assign a name to them. For example, if you wish to allow or forbid your employees to access a different set of websites during working hours than in their free time, you could create the category profiles WORK_CATEGORIES and BASIC_CATEGORIES, for example. For your trainees, you can create the category profile TRAINEE_CATEGORIES, for example. You determine which categories or groups should be used to evaluate websites for each category profile. You can allow or forbid the individual categories or activate the override function for each of the 14 groups.



Pornography, Erotic, Sex: Allowed

Swimwear, Lingerie: Allowed

Set all of them to: Allowed

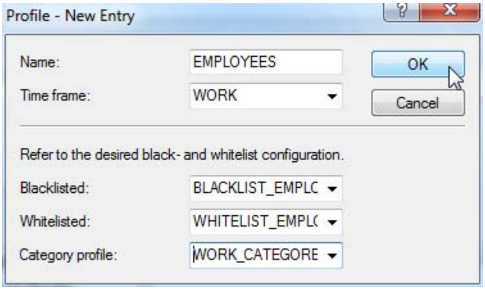
4. You then create your content filter profiles under **Profiles**. A content-filter profile assigns the relevant category profiles and optional blacklists and whitelists to different timeframes. The firewall refers to this content-filter profile.

5. Enter the **Name** EMPLOYEES for the content filter profile EMPLOYEES. Under **Timeframe** select the time when the category profile should apply, e.g. “ALWAYS”. One profile may have several lines with different timeframes. The timeframes in different lines should supplement one another, i.e. if you define a timeframe for WORKTIME it makes sense to also specify a timeframe FREETIME. The timeframes “ALWAYS” and “NEVER” are predefined. You can configure further timeframes (e.g. for staff working time and free time) under:

   LANconfig: Date/Time ▶ General ▶ Timeframe

   WEBconfig: LCOS menu tree ▶ Setup ▶ Time ▶ Timeframe

6. A blacklist or whitelist that you created previously can be selected under **Blacklisted** or **Whitelisted,** e.g. Blacklist_Employees and Whitelist_Employees. You can select the category profile that is to apply for this content filter profile in the selected timeframe under **Category-Profiles,** in this example EMPLOYEES. This completes the settings for the content filter profile EMPLOYEES in the content filter, and you can create further content filter profiles in the same way if needed.



Profile - New Entry

Name: EMPLOYEES

Time frame: WORK

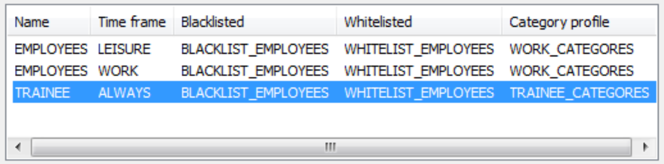
Refer to the desired black- and whitelist configuration.

Blacklisted: BLACKLIST_EMPLC

Whitelisted: WHITELIST_EMPL(

Category profile: WORK_CATEGORE

7. After you have created content filter profiles for your employees and for your trainees, the overview of content filter profiles could look like this:



Name	Time frame	Blacklisted	Whitelisted	Category profile
EMPLOYEES	LEISURE	BLACKLIST_EMPLOYEES	WHITELIST_EMPLOYEES	WORK_CATEGORES
EMPLOYEES	WORK	BLACKLIST_EMPLOYEES	WHITELIST_EMPLOYEES	WORK_CATEGORES
TRAINEE	ALWAYS	BLACKLIST_EMPLOYEES	WHITELIST_EMPLOYEES	TRAINEE_CATEGORES

If you have created different content filter profiles, you will have to modify the settings in the firewall (also see 'Firewall settings for the content filter' →Page 35).

8. A firewall rule must be created in the firewall for each content filter profile. An action object that selects the content-filter profile must be assigned to each firewall rule. One action object may be assigned to several firewall rules.

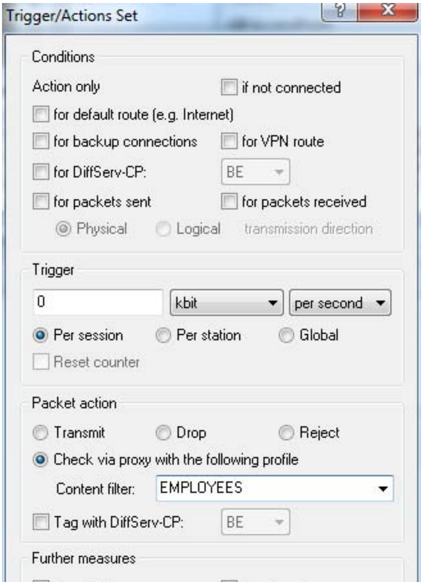
   You can find the action object and the firewall rules under:

   LANconfig: Firewall/QoS ▶ Rules

   WEBconfig: LCOS menu tree ▶ Setup ▶ IP-Router ▶ Firewall

9. The example below shows the settings that you can make in the firewall for your content-filter profile EMPLOYEES:

   Add a new action object with the name "CONTENT FILTER EMPLOYEES" to the **Action-Objects** and, under Actions, assign it to the content-filter profile EMPLOYEES:



Trigger/Actions Set

Conditions

Action only ☐ if not connected

☐ for default route (e.g. Internet)

☐ for backup connections ☐ for VPN route

☐ for DiffServ-CP: BE

☐ for packets sent ☐ for packets received

● Physical ○ Logical transmission direction

Trigger

0 kbit per second

● Per session ○ Per station ○ Global

☐ Reset counter

Packet action

○ Transmit ○ Drop ○ Reject

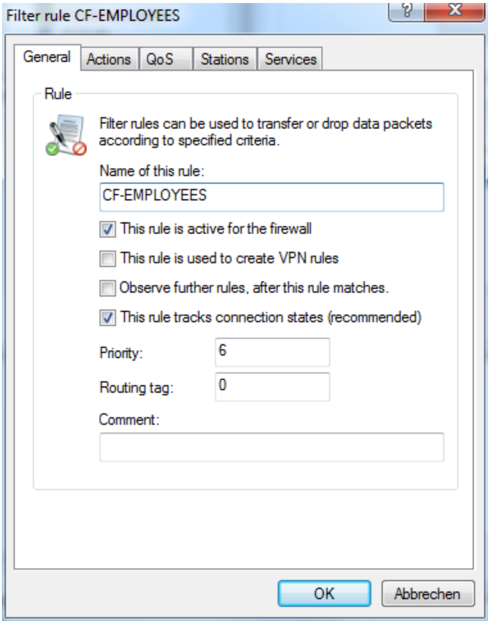
● Check via proxy with the following profile

Content filter: EMPLOYEES

☐ Tag with DiffServ-CP: BE

Further measures

⑩ Define a rule for the action object CONTENT-FILTER-EMPLOYEES:



Filter rule CF-EMPLOYEES

General | Actions | QoS | Stations | Services

Rule

Filter rules can be used to transfer or drop data packets according to specified criteria.

Name of this rule: CF-EMPLOYEES

☑ This rule is active for the firewall

☐ This rule is used to create VPN rules

☐ Observe further rules, after this rule matches.

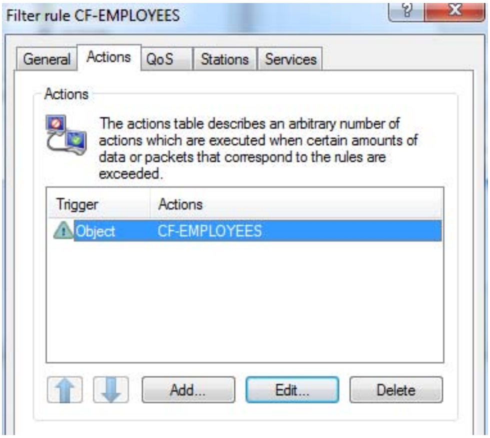
☑ This rule tracks connection states (recommended)

Priority: 6

Routing tag: 0

Comment:

⑪ Under **Actions** assign the action object CONTENT-FILTER-EMPLOYEES to the rule CF-EMPLOYEES:



Filter rule CF-EMPLOYEES

General | Actions | QoS | Stations | Services

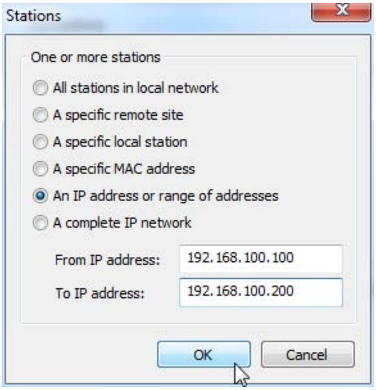
Actions

The actions table describes an arbitrary number of actions which are executed when certain amounts of data or packets that correspond to the rules are exceeded.

Trigger	Actions
Object	CF-EMPLOYEES

⑫ You should now specify further details for the rule, e.g. whether the rule should apply to a certain IP range. To make this setting, click on **Stations** and specify a range of IP addresses to which this rule should apply.

These details in the firewall rule determine the criteria used to allocate users to a certain content-filter profile. The criteria you use here are those which enable you to differentiate between the various user groups.



Stations

One or more stations

○ All stations in local network
○ A specific remote site
○ A specific local station
○ A specific MAC address
● An IP address or range of addresses
○ A complete IP network

From IP address: 192.168.100.100

To IP address: 192.168.100.200

This completes the settings for your content filter profile EMPLOYEES. You can configure your content filter profile TRAINEES in the same way.