LCOS 10.80

LANCOM Content Filter

09/2023

LANCOM
SYSTEMS

Contents

Copyright

© 2023 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

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.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). The license information for the device firmware (LCOS) is available on the device's WEBconfig interface under "Extras > License information". If the respective license demands, the source files for the corresponding software components will be made available on a download server upon request.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (*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-systems.com

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 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 website 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.

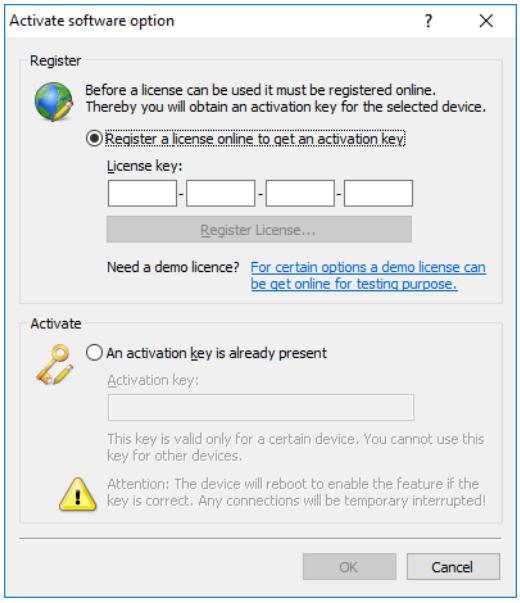
The LANCOM Content Filter operates by checking the IP addresses behind the URLs that are entered. For any given domain it is possible to differentiate according to the path, meaning that specific areas of a URL may be rated differently.

It is not possible for users to avoid the LANCOM Content Filter website rating simply by entering the website's IP address into their browsers. The LANCOM Content Filter checks unencrypted (HTTP) and also encrypted Web pages (HTTPS).

As of LCOS 10.70, the BPjM module is a component of the Content Filter. The BPjM module is published by the German Federal Agency for the Protection of Children and Young People in the Media and blocks domains that may not be made accessible to children and young people in Germany.

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. The included BPjM module is not user-limited, regardless of the number of licensed Content Filter users.

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 **Register 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.



All settings relating to categories are stored in category profiles. You select from predefined main and sub-categories in the LANCOM Content Filter: 59 categories are divided into 14 subject groups such as “Pornography, Nudity”, “Shopping”

or “Illegal Activities”. You can activate or deactivate each of the categories that these groups contain. 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.

Sensible default settings are also set up automatically for the BPjM module. Thus, a default firewall rule exists in the IPv4 or IPv6 firewall with the system object “BPJM” as the target station. Define as source stations the networks that are to be protected by the BPjM module. Activating the rule starts the BPjM module.

The content filter works with a concurrent user model. This model licenses the number of **concurrent** users of the content filter. The content filter maintains a user in its internal user list for 5 minutes only. This makes it possible for a changing selection of users to use the content filter. Your license now checks only the actual number of concurrent users (within the 5-minute period).

2 Requirements for using the LANCOM Content Filter

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

1. The LANCOM Content Filter option has been activated.
2. The firewall must be activated.
3. A firewall rule must select the content filter profile.
4. The selected 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 time span during the day does is not covered by an entry, then access to the Internet goes unchecked during this period.

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

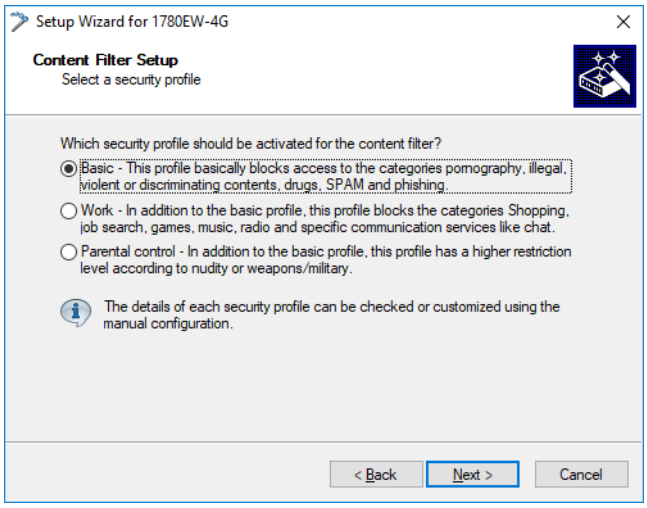
3 Quick start

After the LANCOM Content Filter has been installed, the settings are ready to get you started 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 Content Filter by:

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



3. Select one of the pre-defined security profiles (basic, work, parental control):
   - Basic profile: This profile mainly blocks access to the categories pornography, illegal, violent or discriminatory content, drugs, SPAM and phishing
   - Work profile: 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 profile: 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. The wizard activates the content filter for the time frame ALWAYS.

4 Standard settings in the LANCOM Content Filter

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

Firewall rule

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

Firewall action objects

There are three firewall action objects:

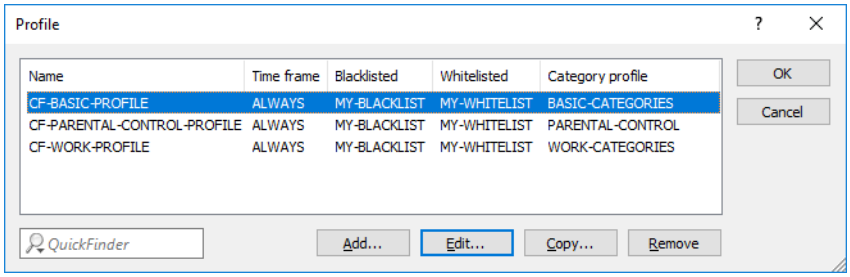
- CONTENT-FILTER-BASIC
- CONTENT-FILTER-WORK
- CONTENT-FILTER-PARENTAL-CONTROL

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.



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

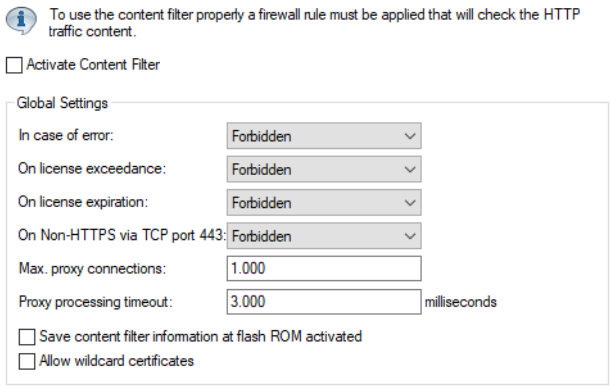
The preset whitelist is named MY-WHITELIST and it is empty. Here you can optionally enter URLs which are to be allowed.

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.

5 General settings

The global settings of the LANCOM Content Filter are located in LANconfig under **Content filter** > **General**:



Activate Content Filter

This is where you can activate the LANCOM Content Filter.

In case of error

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

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 web is blocked entirely.

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 5 minutes.

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 under **Log & Trace** > **General** > **E-mail addresses** > **E-mail for license expiry reminder**).

Here you can specify whether web pages should be blocked or allowed through unchecked after expiry of the license. After the license expires, this setting either allows the user to surf the web without restrictions, or access to the web is blocked entirely.

In order for the reminder to be sent to the specified e-mail address, you must configure the SMTP account.

For non-HTTPS traffic over port 443

Forbidden

Prevents non-HTTPS traffic over port 443.

Allowed

Permits non-HTTPS traffic over port 443

By default the TCP port 443 is reserved exclusively for HTTPS connections.

Some applications that do not use HTTPS still use TCP port 443. In this case, you can also open TCP port 443 for non-HTTPS connections.

If you permit non-HTTPS connections over port 443, the traffic is not further classified and is open for any connection. By default, non-HTTPS connections over port 443 are not permitted.

Max. proxy connections

This setting is for the maximum allowable number of simultaneous proxy connections. This limits the load that can be placed on the system. A notification is sent if this number should be exceeded. You can set the type of notification under **Content filter** > **Options** > **Event notification**.

Proxy processing timeout

Specifies the maximum time in milliseconds that the proxy can take for processing. A timeout error page is displayed if this time is exceeded.

Save Content Filter information to flash ROM activated

If you enable this option, you can additionally save the content filter information to the flash ROM memory of the device.

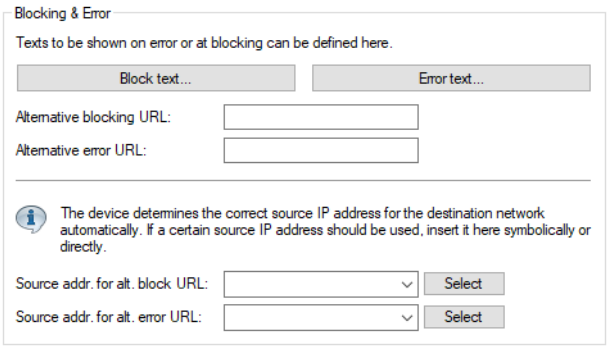
Allow wildcard certificates

With this feature enabled, Web sites with wildcard certificates (consisting of CN entries such as `*.mydomain.com`) are verified using the main domain (`mydomain.com`). Verification is evaluated in this sequence:

- Server name check in the "Client Hello" (depends on the browser used)
- Check of the CN in the SSL certificate that you received
- Entries with wildcards are ignored
- If the CN cannot be verified, the field "Alternative Name"is evaluated.
- DNS reverse lookup of the associated IP address and verification of the host name obtained
- If wildcards are included in the certificate, the main domain is checked instead (corresponds to the above function)
- Verification of the IP address

6 Settings for blocking

You adjust the website-blocking settings here:



LANconfig: **Content filter** > **Blocking / Override** > **Blocking & error**

Command line: **Setup** > **UTM** > **Content-Filter** > **Global-Settings**

Alternative blocking URL:

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 web site. 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 used in the 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

Alternative error URL:

This is where you can enter the address of an alternative URL. In the event of an error, the URL entered here will be displayed instead of the usual web site. 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 used in the error 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

Source addr. for alt. 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.

  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.

Source addr. for alt. error 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.

  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

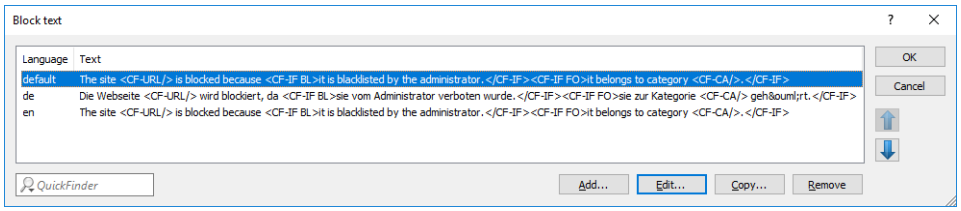
Default:

- Blank

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

6.1 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

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-United States

The country code must match the browser language setting exactly, e.g. “de-DE” must be entered for German (“de” on its own is insufficient). 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 block 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 web site 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 web site 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
- <CF-IF att1 att2> … </CF-IF> to display or hide parts of the HTML document. The 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.
  - OVERRIDEOK: If users have been allowed an override (in this case, the page should display an appropriate button)

Since there are separate text tables for the blocking page and the error page, this attribute only makes sense if you have configured an alternative URL to show on blocking.

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.

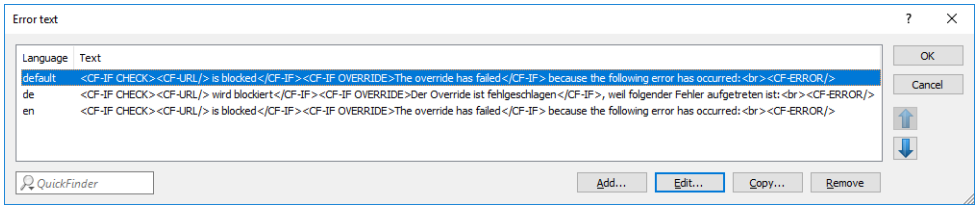
- Example:

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

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

6.2 Error text

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



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-United States

The country code must match the browser language setting exactly, e.g. “de-DE” must be entered for German (“de” on its own is insufficient). 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 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:

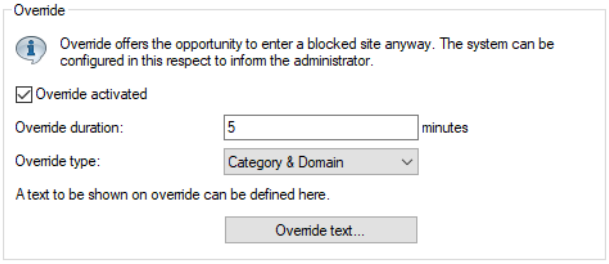
  <CF-URL/> is blocked because an error has occurred: <CF-ERROR/>

7 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 request the forbidden page to be opened. You can configure this feature so that the administrator is notified when the override button is clicked (LANconfig: **Content filter** > **Options** > **Events**).

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. 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:



LANconfig: **Content filter** > **Blocking / Override** > **Override**

Command line: **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 web site 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 web site 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

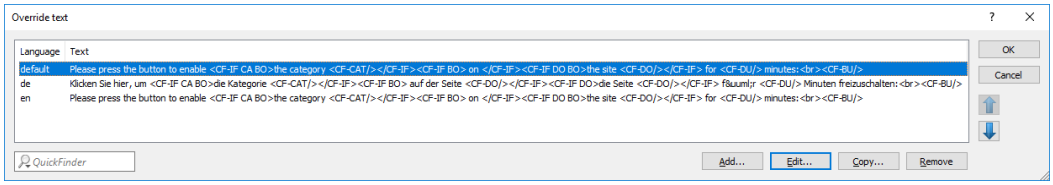
For the duration of the override all URLs in this domain are allowed, irrespective of the categories they belong to.

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.

7.1 Override text

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



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-United States

The country code must match the browser language setting exactly, e.g. “de-DE” must be entered for German (“de” on its own is insufficient). 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 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 web site 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.
- <CF-IF att1 att2> … </CF-IF> to display or hide parts of the HTML document. The attributes are:
  - 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>The categories <CF-CAT/> are</CF-IF><CF-IF BO> in the domain <CF-DO/></CF-IF><CF-IF DO>The domain <CF-DO/> is</CF-IF><CF-IF OK> released for <CF-DU/> minutes. <CF-LI/></CF-IF><CF-IF ERR>Override error: <CF-ERR/></CF-IF>

8 Profiles in the LANCOM Content Filter

Under **Content filter** > **Profiles** you can create content-filter profiles that are used to check web sites 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.

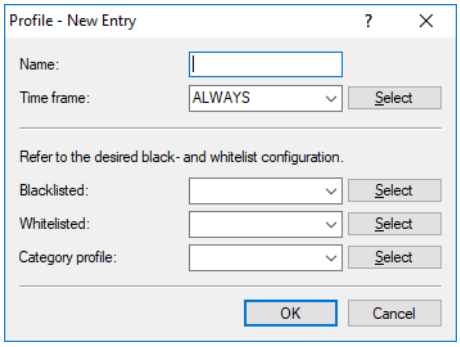
In order to provide different configurations for the various timeframes, several content-filter profile entries are created with the same name. The content-filter profile is thus made up of the sum of all entries with the same name.

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.

8.1 Profiles

The settings for the profiles are to be found here:



LANconfig: **Content filer** > **Profiles** > **Profile**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Profile**

Name

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

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** > **Time frame**

Command line: **Setup** > **Time** > **Timeframe**

One profile may contain several lines with different timeframes.

Possible values:

- Always
- Never
- Name of a timeframe profile

If multiple entries are used for a content-filter profile and their timeframes overlap, then all pages contained in the active entries will be blocked for that period of time. If multiple entries are used for a content-filter profile and a time period remains undefined, access to all web sites will be 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

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

Category profile

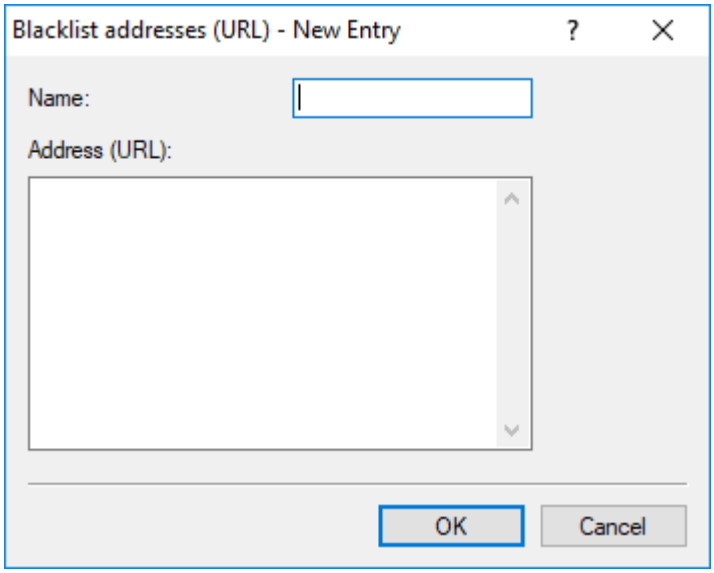
Name of the category profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the category table.

Possible values:

- Name of a category profile
- New name

8.2 Blacklist addresses (URL)

This is where you can configure those web sites that are to be blocked.



LANconfig: **Content files** > **Profiles** > **Blacklist addresses (URL)**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Blacklist**

Name

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

Possible values:

› Blacklist name

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 web sites www.lancom.com, www.lancom.de, www.lancom.eu, www.lancom.es, etc.)

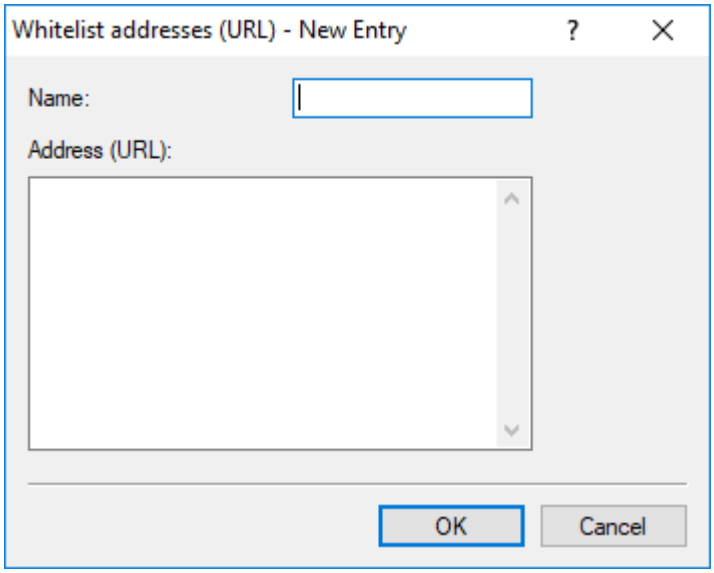
› ? for any one character (e.g. www.lancom.e* encompasses the web sites www.lancom.eu, www.lancom.es)

URLs must be entered **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.

8.3 Whitelist addresses (URL)

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



LANconfig: **Content files** > **Profiles** > **Whitelist addresses (URL)**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Whitelist**

Name

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

Possible values:

- Name of a whitelist

Address (URL)

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

Possible values:

- Valid URL address

The following wildcard characters may be used:

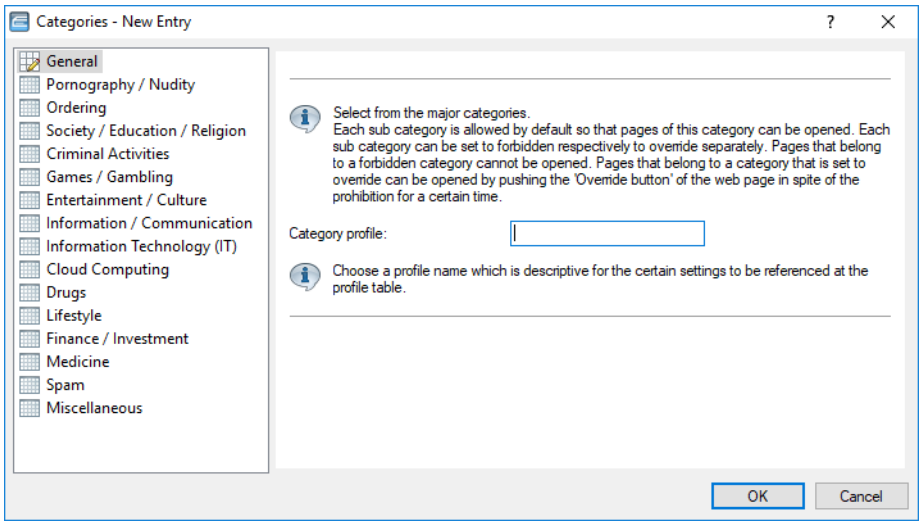
- * for any combination of more than one character (e.g. www.lancom.* encompasses the web sites www.lancom.com, www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? for any one character (e.g. www.lancom.e* encompasses the web sites www.lancom.eu, www.lancom.es)

URLs must be entered **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.

8.4 Category-Profiles

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



LANconfig: **Content filer** > **Profiles** > **Categories**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

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

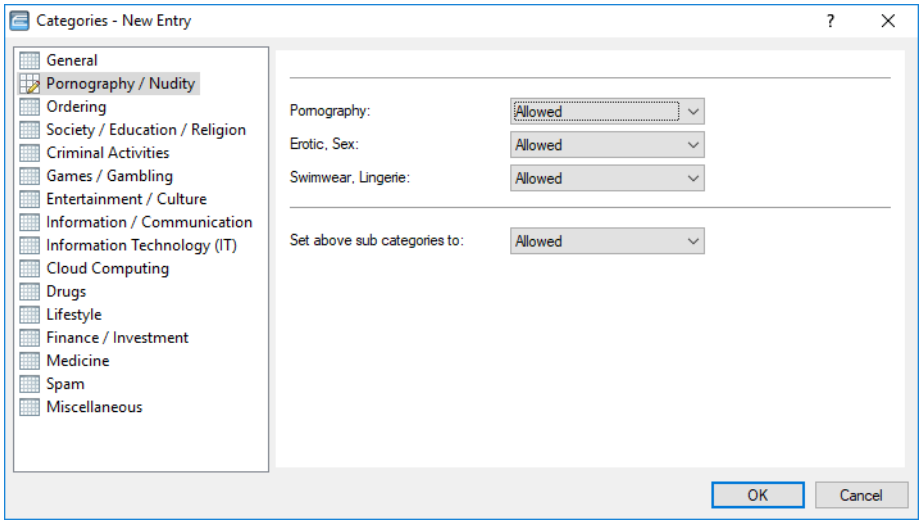
Category settings

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 (IT)
- Cloud applications
- Drugs
- Lifestyle
- Finance / Investment
- Medicine
- Spam

- Miscellaneous



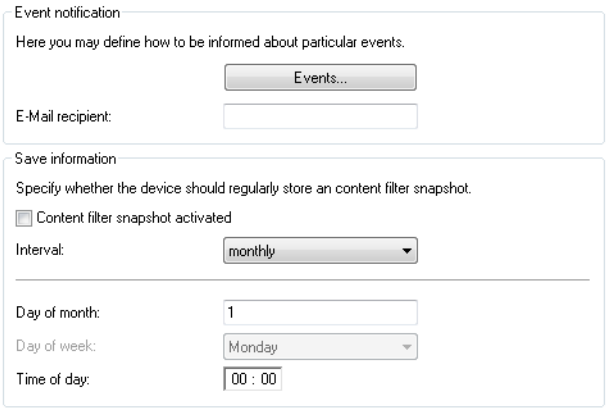
The category profile must then be assigned to a content-filter profile together with a time frame in order to become active.

Possible values:

- Allowed, forbidden, override

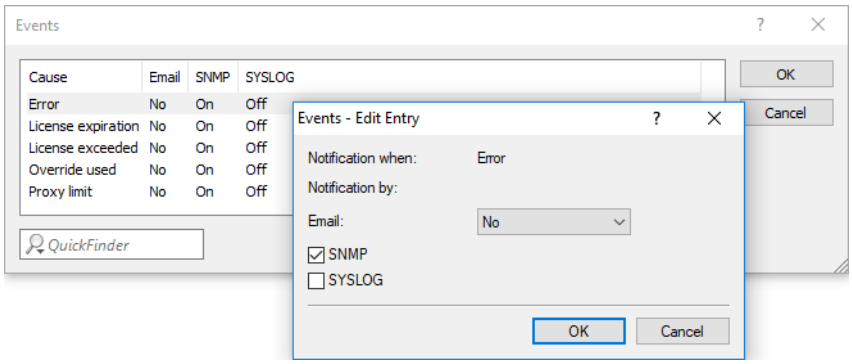
9 Options for the LANCOM Content Filter

Under **Content Filter** > **Options** you determine whether you wish to be notified of events and where LANCOM Content Filter information is to be stored.



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. For different event types you can specify whether messages should be output and, if so, how many.



E-mail

Here, you specify if and how e-mail notification takes place:

- **No**

  No e-mail notification is issued for this event.

- **Immediately**

  Notification occurs when the event occurs.

- **Daily**

  The notification occurs once per day.

Notifications can be sent for the following events:

Error

For SYSLOG: Source “System”, priority “Alert”.

Default: SNMP notification

License expiry

For SYSLOG: Source “Admin”, priority “Alert”.

Default: SNMP notification

License exceeded

For SYSLOG: Source “Admin”, priority “Alert”.

Default: SNMP notification

Override applied

For SYSLOG: Source “Router”, priority “Alert”.

Default: SNMP notification

Proxy limit

For SYSLOG: Source “Router”, priority “Info”.

Default: SNMP notification

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 specified.

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

Day of month

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

- 1-31

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

Day of week

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

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

Time of day:

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

- Format HH:MM (default: 00:00)

10 Additional settings for the LANCOM Content Filter

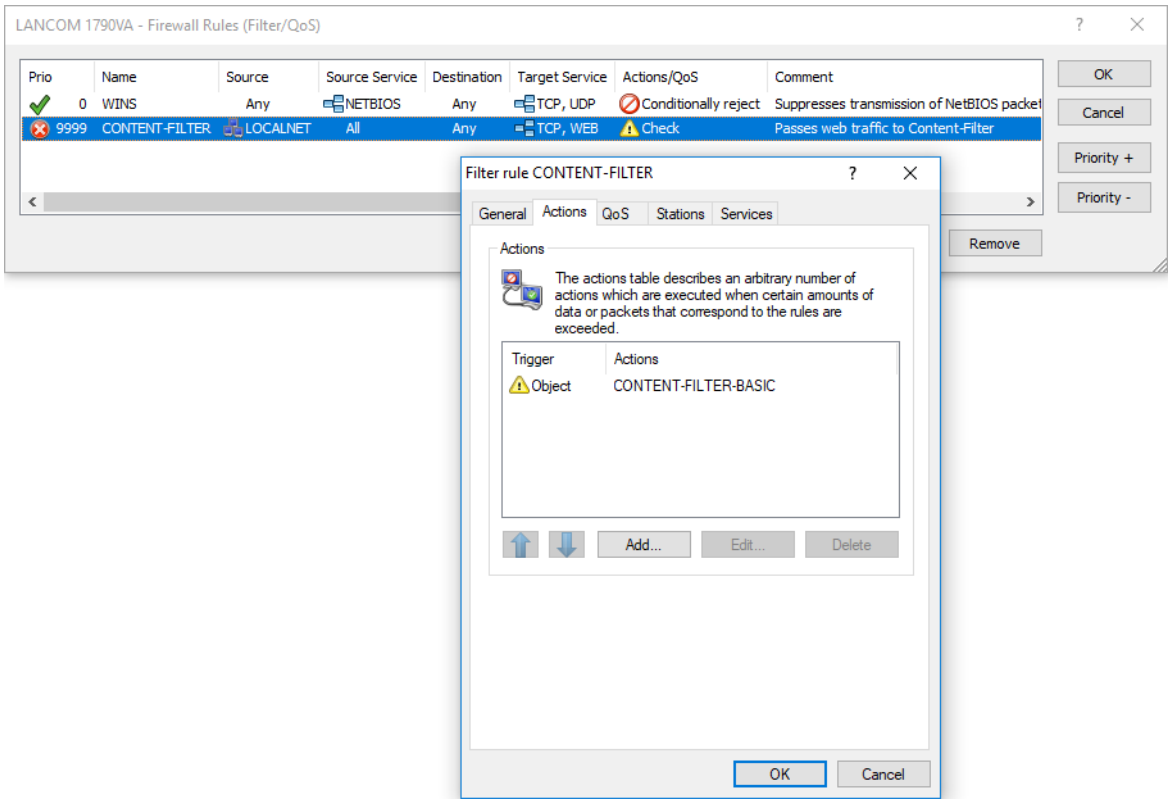
10.1 Firewall settings for the content filter

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

LANconfig: **Firewall/QoS** > **General**

Command line: **Setup** > **IP-Router** > **Firewall**

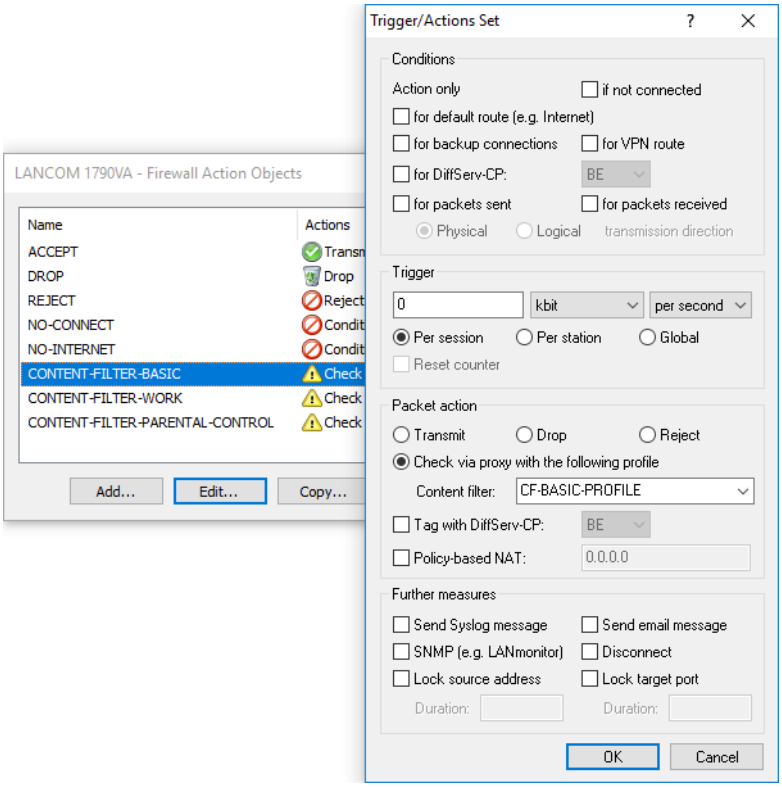
In the default configuration, you will find the firewall rule CONTENT-FILTER that refers to the action object CONTENT-FILTER-BASIC:



The firewall rule should be limited to the target services HTTP and HTTPS so that only outgoing HTTP and HTTPS 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:



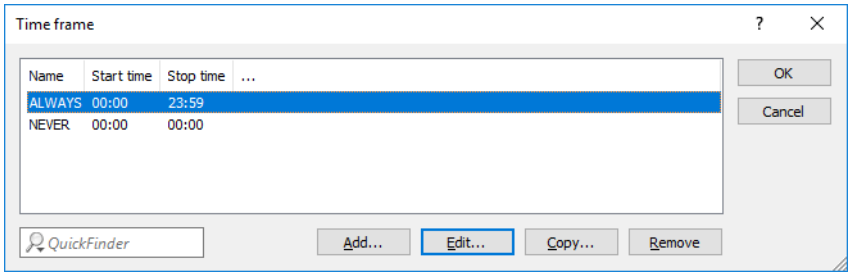
Example: When a web page is accessed, the data packets pass through the firewall and are processed by the rule CONTENT-FILTER. The action object CONTENT-FILTER-BASIC checks the data packets using the content-filter profile CONTENT-FILTER-BASIC.

10.2 Timeframe

Time frames are used with the Content Filter to define the times when the content-filter profiles apply. One profile may contain several lines with different timeframes. Different lines in a timeframe should complement one another, i.e. if you specify WORKTIME you will should probably specify a timeframe called FREETIME to cover the time outside of working hours.

Time frames can also be used to prevent a WLAN SSID from being broadcast permanently. This can be added to the logical WLAN settings.

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



LANconfig: **Date & time** > **General** > **Time frame**

Command line: **Setup** > **Time** > **Timeframe**

Name

Enter the name of the time frame for referencing from the content-filter profile or by a WLAN SSID. Several entries with the same name result in a common profile.

Possible values:

- Name of a timeframe

Start

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

Possible values:

- Format HH:MM (default: 00:00)

Stop

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

Possible values:

- Format HH:MM (default: 23:59)

A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

Weekdays

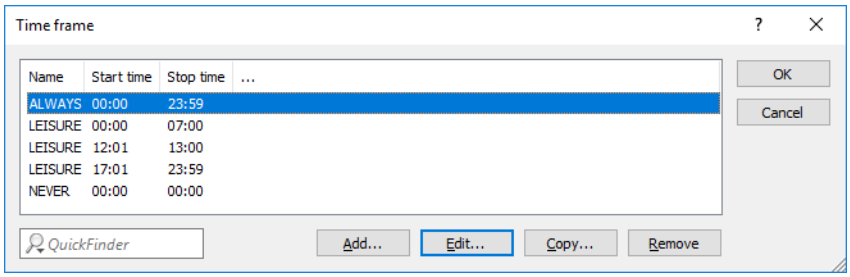
Here you select the weekday on which the timeframe is to be valid.

Possible values:

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

The holidays are set under **Date & Time** > **General** > **Public holidays**.

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



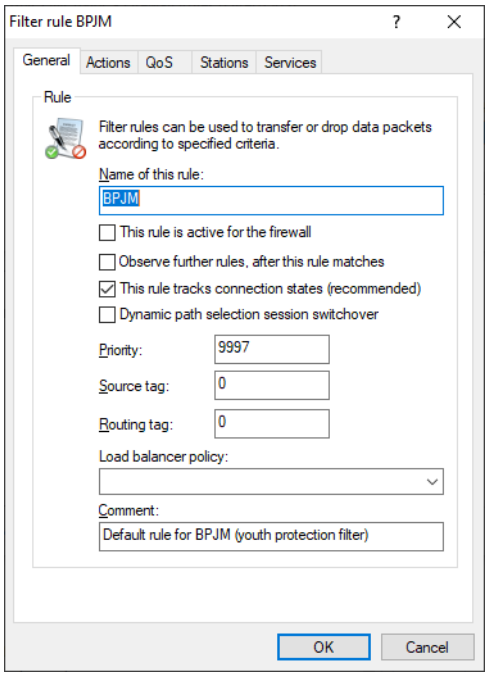
11 BPjM module

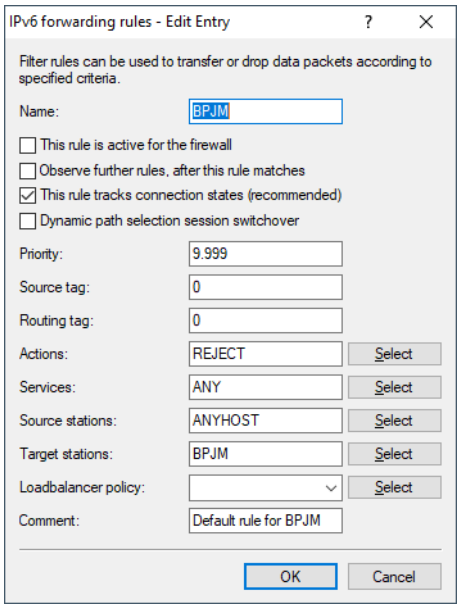
The BPjM module was setup by Germany's Federal Review Board for Media Harmful to Minors (BPjM) and blocks websites that should not be accessible to children and young people. This feature is particularly relevant for schools and educational institutions with underage students. DNS-Domains with content that is officially classified as harmful to minors cannot be accessed by the relevant target group. This list is guaranteed to be automatically updated and extended on a regular basis. The BPjM module blocks DNS-Domains that are listed on the official website of the Federal Review Board for Media Harmful to Minors (BPjM) in Germany. Blocking by category and overrides (allow) are not available.

The BPjM module is available as part of the LANCOM Content Filter option or separately via the LANCOM BPjM Filter software option.

The IPv4 or IPv6 firewalls implement this feature with a default firewall rule that can be activated and configured for each network. For example, it is possible to equip only the students' network with this filter, but exclude other networks from it.

The IPv6 firewall features a new default rule BPJM, which is deactivated by default with the system object "BPJM" as the destination station. A similar rule is available in the IPv4 firewall. The networks to be protected by the BPjM module are specified as source stations.





Further settings can be found in LANconfig under **Miscellaneous Services** > **Services** > **BPjM filter**.

Source address

Source address used by the BPjM module to access the server for BPjM signature updates.

11.1 Recommendations for use

If content filters and BPJM filters are to be used together, both rules must be configured with different priorities so that they are run through one after the other.

Likewise, for the first rule, care must be taken to ensure that the item “Observe further rules, after this rule matches” is activated.

In rare cases, the BPJM module may block desired domains because only (DNS) domains and not URL directory levels can be checked due to TLS. In this case, these desired domains can be added to the “BPJM Allow list”, e.g. *.example.com.

The LANCOM router must serve as DNS server or DNS forwarder in the network, i.e. clients in the local network must use the router as DNS server. In addition, the direct use of DNS-over-TLS and DNS-over-HTTPS (possibly browser-internal) with external DNS servers by clients must be prevented.

This can be achieved as follows:

- The DHCP server must distribute the router's IP address as the DNS server (set up by default by the Internet Wizard).
- Set up firewall rules that prevent direct use of external DNS servers, for example. by blocking outgoing port 53 (UDP) for clients from the corresponding source network.
- Setting up firewall rules that prevent direct use of external DNS servers supporting DNS-over-TLS, e.g. by blocking outgoing port 853 (TCP) for clients from the corresponding source network.
- Disabling DNS-over-HTTPS (DoH) in the browser.

Notes on synchronizing the firewall's DNS database:

Because the firewall learns its information from client DNS requests, in certain situations the DNS database may not yet be complete. This can happen in the following situations:

- A new firewall rule is added, but the client still has a DNS record cached.
- Shortly after the router reboots and the client still has a DNS record cached.

In these cases, clearing the DNS cache on the client, rebooting the client, or timing out the DNS record on the client will help.

If different DNS names resolve to the same IP address, then they cannot be distinguished. In this case, the first rule that references one of these DNS names always applies. This should not be a problem with large service providers. However, it could occur with small websites hosted by the same provider.