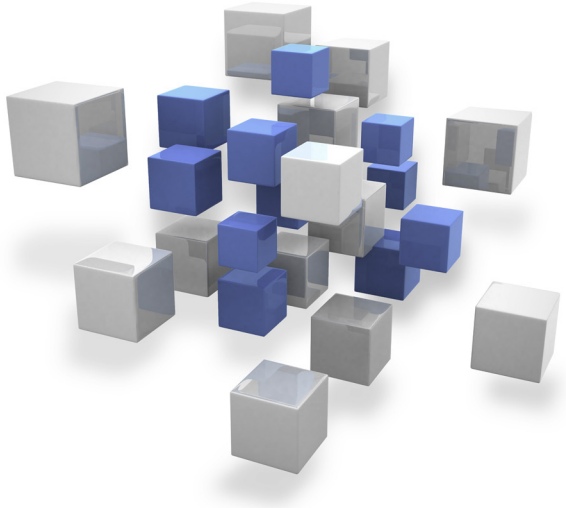

LANCOM Content Filter Option

Optimal protection against network abuse

The LANCOM Content Filter provides an effective solution that protects networks from abuse, prevents the inappropriate use of bandwidth, and blocks malware downloads. Blocking undesirable and illegal Internet content protects business integrity and it minimizes liability risks at the same time.

- Category-based web filter
- Time- and profile-based configuration
- Extensive usage statistics
- Category-based overrides for web pages and sites
- Additive licenses for 10, 25 or 100 users
- Available for LANCOM VPN routers, central-site VPN gateways, and WLAN controllers
- Simply upgrade your existing device and save on hardware components

LANCOM Content Filter Option

Protection against network abuse

The LANCOM Content Filter ensures that network bandwidth is completely reserved for business operations, while websites with spyware, phishing, viruses, etc., are securely blocked. The Content Filter uses a database-driven web-filter technology, with an external evaluation server that checks the requested sites online and rates the actual content. The administrator is free to configure which thematic categories are blocked and which are accessible. Three default security profiles—basic, company, protection of minors—make it quick and easy to introduce this solution.

Customized time- and profile-based configuration

Using the LANCOM Content Filter, the permission to access websites from within a network can be freely configured according to the time and personal data. For example, content that is blocked during core business hours can be free to access during the lunch break. It is also possible to create profiles for individual users so that, for example, Internet content that is relevant to their work is unlocked for the persons concerned.

Comprehensive statistics for a clear overview

The LANCOM Content Filter provides an extensive range of statistics. For example, you can create top-10 lists for any period of time to indicate the access statistics for allowed sites, blocked sites, and override URLs. Ratings can be carried out according to categories. Statistics are not related to individual persons, which is important for the adherence to strict privacy guidelines.

Category-based overrides for websites

The override button permits temporary access to blocked websites. This enables access to blocked URLs for a limited period of time without having to make changes to the configuration. Overrides can be activated for each category and are optionally logged by e-mail, SYSLOG and SNMP. This is a useful feature when users have justifiable reasons to want or need to access certain websites.

Effective protection for large and small

The Content Filter is licensed by the number of users. The LANCOM device determines the number of users by counting the IP addresses that receive filtered content. By licensing according to size you can adjust precisely to your actual network and, if necessary, you can conveniently handle a growth in demand.

Easy upgrades

The LANCOM software options turn a simple network into a customized and cost-efficient solution that meets your individual needs. Simply install them on your existing hardware and you upgrade your network with the desired feature. The advantage: No additional hardware components are required. The costs and the administration overhead of the entire network are reduced. Genuine added value comes in terms of the system's future viability, because the options transform a network into a customized and scalable networking solution.

LANCOM
Systems

LANCOM Content Filter Option

Content Filter	
URL filter database/rating server*	Worldwide, redundant rating servers from IBM Security Solutions for querying URL classifications. Database with over 100 million entries covering about 10 billion web pages. Web crawlers automatically search and classify web sites to provide nearly 150,000 updates per day: They use text classification by optical character recognition, key word searches, classification by word frequency and combinations, web-site comparison of text, images and page elements, object recognition of special characters, symbols, trademarks and prohibited images, recognition of pornography and nudity by analyzing the concentration of skin tones in images, by structure and link analysis, by malware detection in binary files and installation packages
URL check*	Database based online check of web sites (HTTP/HTTPS). HTTPS websites are checked based on DNS names of HTTPS server certificates or based on “Reverse DNS lookup“ of IP addresses.
Categories/category profiles*	Filter rules can be defined in each profile by collecting category profiles from 58 categories, for example to restrict Internet access to business purposes only (limiting private use) or by providing protection from content that is harmful to minors or hazardous content (e.g. malware sites). Clearly structured selection due to the grouping of similar categories. Content for each category can be allowed, blocked, or released by override
Override**	Each category can be given an optional manual override that allows the user to access blocked content on a case-by-case basis. The override operates for a limited time period by allowing the category or domain, or a combination of both. Optional notification of the administrator in case of overrides
Black-/whitelist	Lists that are manually configured to explicitly allow (whitelist) or block (blacklist) web sites for each profile, independent of the rating server. Wildcards can be used when defining groups of pages or for filtering sub pages
Profiles	Timeframes, blacklists, whitelists and categories are collected into profiles that can be activated separately for content-filter actions. A default profile with standard settings blocks racist, pornographic, criminal, and extremist content as well as anonymous proxies, weapons/military, drugs, SPAM and malware
Time frames	Timeframes can be flexibly defined for control over filtering depending on the time of day or weekday, e.g. to relax controls during break times for private surfing
Flexible firewall action	Activation of the content filter by selecting the required firewall profile that contains content-filter actions. Firewall rules enable the flexible use of your own profiles for different clients, networks or connections to certain servers
Individual display pages (for blocked, error, override)	Response pages displayed by the content filter in case of blocked sites, errors or overrides can be custom designed. Variables enable the inclusion of current information such as the category, URL, and rating-server categorization. Response pages can be issued in any language depending on the language set in the user's web browser
Redirection to external pages	As an alternative to displaying the device's own internal response pages to blockings, errors or overrides, you can redirect to external web servers
License management	Automatic notification of license expiry by e-mail, LANmonitor, SYSLOG or SNMP trap. Activation of license renewal at any time before expiry of the current license (the new licensing period starts immediately after expiry of the current license)
Statistics	Display of the number of checked and blocked web pages by category in LANmonitor. Logging of all content-filter events in LANmonitor; log file created daily, weekly or monthly. Hit list of the most frequently called pages and rating results. Analysis of the connection properties; minimum, maximum and average rating-server response time
Notifications	Messaging in case of content-filter events optionally by e-mail, SNMP, SYSLOG or LANmonitor
Wizard for typical configurations	Wizard sets up the content filters for a range of typical scenarios in a few simple steps, including the creation of the necessary firewall rules with the corresponding action
*) Note	Categorization is maintained by IBM. Neither IBM or LANCOM can guarantee full accuracy of the categorization.
**) Note	The Override function is only available for HTTP websites.

Suitable for	
LANCOM 831A	max. 25 users
LANCOM 1631E	max. 25 users
LANCOM 19xx	max. 500 users
LANCOM 178x	max. 100 users
LANCOM IAP-(321)-3G	max. 100 users
LANCOM IAP-4G	max. 100 users
LANCOM OAP-3G	max. 100 users

LANCOM Systems

LANCOM Content Filter Option

Suitable for	
LANCOM 88x VoIP	max. 100 users
LANCOM WLC 4006(+)	max. 100 users
LANCOM WLC 4025+	max. 400 users
LANCOM WLC 4100	max. 400 users
LANCOM 7100(+) VPN	max. 400 users
LANCOM 9100(+) VPN	max. 400 users
Item number(s)	
LANCOM Content Filter +10 user, 1 year option	61590
LANCOM Content Filter +25 user, 1 year option	61591
LANCOM Content Filter +100 user, 1 year option	61592
LANCOM Content Filter +10 user, 3 year option	61593
LANCOM Content Filter +25 user, 3 year option	61594
LANCOM Content Filter +100 user, 3 year option	61595

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Wuerselen I Germany I E-Mail info@lancom-systems.com