LANCOM Content Filter Option

- **Handbuch**
- **Manual**

LANCOM
Systems

LANCOM Content-Filter

LANCOM Systems

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Mai 2010

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Der LANCOM Content-Filter ist ein Filter für Web-Seiten im Internet. Sie haben die Möglichkeit, bestimmte Seiten grundsätzlich zu erlauben, zu verbieten und Seiten von einem Online-Server anhand vordefinierter Kategorien bewerten zu lassen.

Der Einsatz der LANCOM Content-Filter Option kann je nach Einsatzort bestimmten Einschränkungen durch Gesetze oder Richtlinien zum Datenschutz sowie betrieblichen Vereinbarungen unterliegen. Bitte prüfen Sie vor der Inbetriebnahme der LANCOM Content-Filter Option die jeweils geltenden Gesetze, Richtlinien oder Vereinbarungen.

Sicherheitseinstellungen

Für einen sicheren Umgang mit Ihrem Produkt empfehlen wir Ihnen, sämtliche Sicherheitseinstellungen (z. B. Firewall, Verschlüsselung, Zugriffsschutz) vorzunehmen, die nicht bereits zum Zeitpunkt des Kaufs des Produkts aktiviert waren. Der LANconfig-Assistent 'Sicherheitseinstellungen' unterstützt Sie bei dieser Aufgabe. Weitere Informationen zum Thema Sicherheit finden Sie auch im Kapitel 'Sicherheitseinstellungen'.

Zusätzlich bitten wir Sie, sich auf unserer Internet-Seite www.lancom.de über technische Weiterentwicklungen und aktuelle Hinweise zu Ihrem Produkt zu informieren und ggf. neue Software-Versionen herunterzuladen.

An der Erstellung dieser Dokumentation …

… haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:
info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf „häufig gestellte Fragen ('FAQs')". Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools

und Dokumentation stehen für Sie jederzeit zum Download bereit. Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

DE

Hinweis-Symbole	
	Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.
	Wichtiger Hinweis, der beachtet werden sollte.
	Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

Inhalt

DE

1 Aktivieren der LANCOM Content-Filter Option

In diesem Kapitel erfahren Sie, wie Sie die LANCOM Content-Filter Option auf Ihrem LANCOM aktivieren. Die Aktivierung erfolgt in vier Schritten:

① Sicherstellen der Installations-Voraussetzungen

② Online-Registrierung

③ Eingabe des Aktivierungsschlüssels

④ Überprüfen der Aktivierung

1.1 Installations-Voraussetzungen

Der Einsatz der LANCOM Content-Filter Option kann je nach Einsatzort bestimmten Einschränkungen durch Gesetze oder Richtlinien zum Datenschutz sowie betrieblichen Vereinbarungen unterliegen. Bitte prüfen Sie von Inbetriebnahme der LANCOM Content-Filter Option die jeweils geltenden Gesetze, Richtlinien oder Vereinbarungen.

1.1.1 Systemvoraussetzungen

Vergewissern Sie sich, dass Sie alle Voraussetzungen für den erfolgreichen Betrieb der LANCOM Content-Filter Option erfüllt haben:

- LANCOM Gerät mit der Option die LANCOM Content-Filter Option zu aktivieren.
- Lizenznachweis für die LANCOM Content-Filter Option.

1.1.2 Lieferumfang

Vergewissern Sie sich, dass das Optionspaket folgende Komponenten enthält:

- Lizenznachweis mit aufgedruckter Lizenznummer
- Handbuch

1.1.3 Konfigurations-Rechner mit Windows-Betriebssystem

Sie benötigen für die Installation der LANCOM Content-Filter Option mit LANconfig einen Rechner mit einem Windows-Betriebssystem. Alternativ kann die Aktivierung auch über WEBconfig erfolgen.

Dieser Rechner muss Zugriff auf den zu konfigurierenden LANCOM haben. Der Zugriff kann entweder über LAN oder über die Fernkonfiguration erfolgen.

1.1.4 Aktuelles LANconfig

Die jeweils aktuelle Version von LANconfig und LANmonitor finden Sie auf der LANCOM Systems Homepage unter www.lancom.de/download/. Es empfiehlt sich in jedem Fall, diese Programme vor der weiteren Installation zu aktualisieren.

1.1.5 Aktuelle Firmware im LANCOM

Aktuelle Firmware-Updates finden Sie auf der LANCOM Systems Website unter www.lancom.de/download/. Suchen Sie Ihr Gerät in der Geräteliste aus und laden Sie die Datei mit der passenden Firmware auf Ihren Rechner herunter.

Nähere Informationen zur Aktualisierung der Firmware finden Sie in der Dokumentation Ihres LANCOM-Gerätes.

1.2 Online-Registrierung

Zur Aktivierung der LANCOM Content-Filter Option im LANCOM benötigen Sie einen Aktivierungsschlüssel.

Beachten Sie bitte: Der Aktivierungsschlüssel liegt dem Paket nicht bei, sondern wird Ihnen bei der Online-Registrierung mitgeteilt.

Der LANCOM Content-Filter Option liegt ein Lizenznachweis bei. Auf diesem ist eine Lizenznummer abgedruckt. Mit der Lizenznummer können Sie sich einmalig bei LANCOM Systems registrieren und erhalten dann einen Aktivierungsschlüssel.

Eine erfolgreiche Online-Registrierung entwertet die verwendete Lizenznummer Ihrer LANCOM Content-Filter Option. Der hieraus gewonnene Aktivierungsschlüssel ist ausschließlich auf dem per Seriennummer angegebenen LANCOM Gerät verwendbar! Vergewissern Sie sich, dass Sie die LANCOM Content-Filter Option tatsächlich nur auf dem angegebenen Gerät installieren wollen. Ein späterer Wechsel auf ein anderes Gerät ist ausgeschlossen.

Erforderliche Registrierungsdaten

Zur Online-Registrierung halten Sie bitte folgende Daten bereit:

- Genaue Bezeichnung der Software-Option
- Die Lizenznummer (vom Lizenznachweis)
- Seriennummer Ihres zu aktivierenden LANCOMs (befindet sich auf der Gehäuseunterseite)
- Ihre Kundendaten (Firma, Name, Anschrift, E-Mail-Adresse).

Die Registrierung ist auch anonym, also ohne Angabe persönlicher Daten, möglich. Zusätzliche Informationen erleichtern uns eine Unterstützung im Support- und Servicefall. Alle Daten werden selbstverständlich streng vertraulich behandelt.

Online-Eingabe der Registrierungsdaten

① Starten Sie einen Webbrowser und gehen Sie auf die LANCOM Systems Website unter www.lancom.de/routeroptionen.

② Geben Sie die erforderlichen Daten ein und folgen Sie den weiteren Anweisungen. Nach Eingabe aller Daten werden Ihnen der Aktivierungsschlüssel für Ihr Gerät sowie Ihre Kundendaten übermittelt. Wenn Sie Ihre E-Mail-Adresse angegeben haben, werden Ihnen die Daten einschließlich des Aktivierungsschlüssels per E-Mail zugesandt. Die Online-Registrierung ist damit beendet.

Heben Sie den Aktivierungsschlüssel gut auf! Möglicherweise benötigen Sie ihn später zum erneuten Aktivieren der LANCOM Content-Filter Option etwa nach einer Reparatur.

Hilfe im Problemfall

Bei Problemen mit der Registrierung Ihrer Software-Option wenden Sie sich bitte per E-Mail an optionsupport@lancom.de.

1.3 Aktivieren der LANCOM Content-Filter Option

Die Aktivierung der LANCOM Content-Filter Option ist sehr einfach.

- In LANconfig markieren Sie des gewünschte Gerät (durch einfachen Mausklick auf den Eintrag) und wählen den Menübefehl **Gerät ▶ Software-Option aktivieren**. Klicken Sie alternativ den Geräteeintrag mit

DE

der rechten Maustaste und wählen Sie im Kontext-Menü den Eintrag **Software-Option aktivieren**.

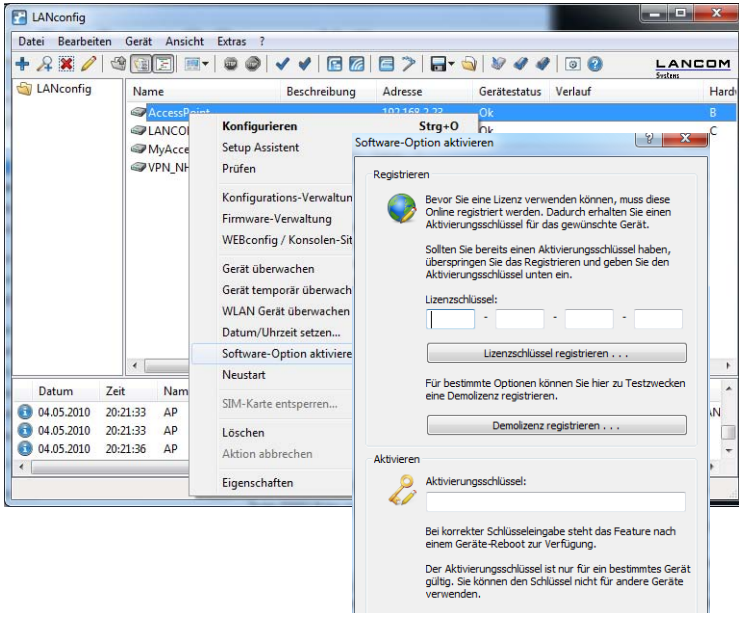
- Unter WEBconfig wählen Sie den Menübefehl **Extras ▶ Software-Option aktivieren**.

  Geben Sie im folgenden Fenster den Aktivierungsschlüssel ein, den Sie über oben genannte Online-Registrierung erworben haben. Das Gerät startet anschließend automatisch neu.

- An der Kommandozeile (z.B. Telnet) benutzen Sie den Befehl **feature**, gefolgt vom Aktivierungsssschlüssel:

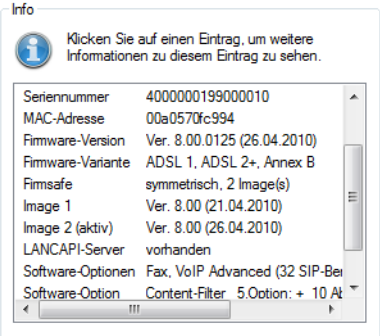
  `feature <Aktivierungsssschlüssel>`

Bitte beachten Sie, dass die Aktivierung der LANCOM Content-Filter Option für einen bestimmten Zeitraum gültig ist. Sie können sich rechtzeitig vor Ablauf der Lizenz eine E-Mail zusenden lassen (WEBconfig: **LCOS-Menübaum ▶ Setup ▶ Config ▶ Lizenzablauf-Email**).



1.4 Überprüfen der Aktivierung

Die erfolgreiche Aktivierung der LANCOM Content-Filter Option können Sie überprüfen, indem Sie beim ausgewähltem Gerät in LANconfig den Menübefehl **Gerät** ▶ **Eigenschaften** auswählen. Im Eigenschaften-Fenster sehen Sie im Register 'Info' eine Liste der aktiven Software-Optionen.



Wenn die Aktivierung erfolgreich war, können Sie mit der Konfiguration des LANCOM Content-Filters fortfahren.

2 Konfiguration des LANCOM Content- Filters

2.1 Einleitung

DE

Mit dem LANCOM Content- Filter können Sie bestimmte Inhalte in Ihrem Netzwerk filtern und dadurch den Zugriff auf z.B. illegale, gefährliche oder anstößige Internetseiten verhindern. Weiterhin können Sie das private Surfen auf bestimmten Seiten während der Arbeitszeit unterbinden. Das steigert nicht nur die Produktivität der Mitarbeiter und die Sicherheit des Netzwerks, sondern sorgt auch dafür, dass die volle Bandbreite auschließlich für Geschäftsprozesse zur Verfügung steht.

Der LANCOM Content- Filter ist ein intelligenter Content- Filter und arbeitet dynamisch. Er kontaktiert einen Bewertungsserver, der gemäß den von Ihnen ausgewählten Kategorien die Bewertung der Internetseiten zuverlässig und korrekt vornimmt.

Die Funktion des LANCOM Content- Filters basiert auf der Überprüfung der IP-Adressen, die anhand der eingegebenen URL ermittelt werden. Innerhalb einer Domain wird bei vielen Seiten außerdem nach dem Pfad unterschieden, so dass bestimmte Bereiche einer URL unterschiedlich bewertet werden können.

Die Anwender können die Prüfung der aufgerufenen Webseiten durch den LANCOM Content- Filter nicht umgehen, indem sie die IP- Adresse zu einer Webseite ermitteln und diese in den Browser eingeben.
Der LANCOM Content- Filter prüft nur unverschlüsselte Webseiten über HTTP.

Die von Ihnen erworbene Lizenz für den LANCOM Content Filter gilt für eine bestimmte Anzahl Benutzer und einen bestimmten Zeitraum (jeweils für ein Jahr oder drei Jahre). Sie werden rechtzeitig über den Ablauf Ihrer Lizenz informiert. Die Anzahl der aktuellen Benutzer wird im Gerät geprüft, dabei werden die Benutzer über die IP- Adresse identifiziert. Sie können das Verhalten bei Lizenzüberschreitung einstellen: Entweder wird der Zugriff verboten oder es wird eine ungeprüfte Verbindung hergestellt.

Sie können den LANCOM Content Filter auf jedem Router testen, der diese Funktion unterstützt. Hierfür müssen Sie für jedes Gerät einmalig eine zeitlich befristete 30-Tage Demo- Lizenz aktivieren. Demo-Lizenzen werden direkt aus LANconfig heraus erstellt. Klicken Sie mit der rechten Maustaste auf das Gerät, wählen Sie im Kontextmenü den

Eintrag **Software-Option aktivieren** und im folgenden Dialog die Schaltfläche **Demo-Lizenz**. Sie werden automatisch mit der Webseite des LANCOM-Registrierungsservers verbunden, auf der Sie die gewünschte Demo-Lizenz auswählen und für das Gerät registrieren können.

Über die Kategorieprofile speichern Sie alle Einstellungen bezüglich der Kategorien. Dabei wählen Sie aus vordefinierte Haupt- und Unterkategorien in Ihrem LANCOM Content-Filter: 58 Kategorien sind zu 14 Gruppen thematisch zusammengefasst, z.B. "Pornographie/Nacktheit", "Einkaufen" oder "Kriminelle Aktivitäten". Für jede dieser Gruppen lassen sich die enthaltenen Kategorien aktivieren oder deaktivieren. Die Unterkategorien für "Pornographie/Nacktheit" sind z.B. "Pornographie/Erotik/Sex", "Bademoden/Dessous".

Zusätzlich kann der Administrator bei der Konfiguration für jede dieser Kategorien die Option des Override aktivieren. Bei aktivem Override kann der Benutzer den Zugriff auf eine verbotene Seite durch einen Klick auf eine entsprechende Schaltfläche für eine bestimmte Zeitspanne freischalten – allerdings erhält der Administrator in diesem Fall eine Benachrichtigung per E-Mail, Syslog und/oder SNMP-Trap.

Mit dem von Ihnen erstellten Kategorieprofil, der Whitelist und der Blacklist können Sie ein Content-Filter-Profil anlegen, welches über die Firewall gezielt Benutzern zugeordnet werden kann. Beispielsweise können Sie das Profil

"Mitarbeiter_Abteilung_A" anlegen, welches dann allen Computern der entsprechenden Abteilung zugeordnet wird.

Bei der Installation des LANCOM Content-Filter werden sinnvolle Standardeinstellungen automatisch eingerichtet, die für den ersten Start nur aktiviert werden müssen. In weiteren Schritten können Sie das Verhalten des LANCOM Content-Filters weiter an Ihren speziellen Anwendungsfall anpassen.

2.2 Voraussetzungen für die Benutzung des LANCOM Content-Filters

Folgende Voraussetzungen müssen erfüllt sein, damit Sie den LANCOM Content-Filter benutzen können:

1. Die Firewall muss aktiviert sein und mit einer entsprechenden Firewall-Regel das Content-Filter-Profil auswählen.
2. Das Content-Filter-Profil muss für jeden Zeitraum das Tages ein Kategorieprofil und nach Wunsch eine White- und/oder Blacklist festlegen. Um die verschiedenen Zeiträume abzudecken, kann ein Content-Filter-Profil aus mehreren Einträgen bestehen.

   Wird ein bestimmter Zeitraum des Tages nicht über einen Eintrag abgedeckt, so ist in diesem Zeitraum ein unprüfter Zugriff auf die Webseiten möglich.

Wenn das Content-Filter-Profil nachträglich umbenannt wird, muss die Firewallregel ebenfalls angepasst werden.

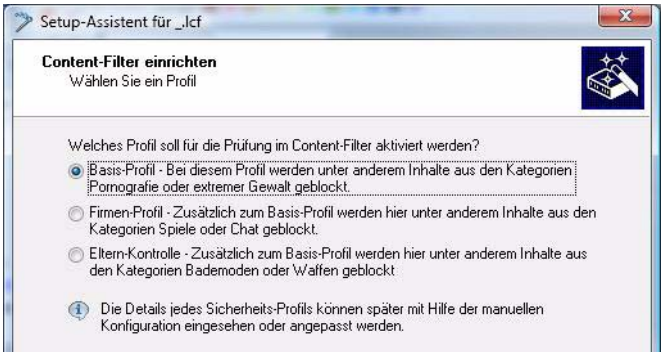
2.3 Quickstart

Nach der Installation des LANCOM Content-Filter sind alle Einstellungen für eine schnelle Inbetriebnahme vorbereitet.

Der Betrieb des LANCOM Content-Filter kann durch die Datenschutzrichtlinien in Ihrem Land oder Betriebsvereinbarungen in Ihrem Unternehmen eingeschränkt sein. Bitte prüfen Sie vor Inbetriebnahme die geltenen Regelungen.

Aktivieren Sie den LANCOM Content-Filter in den folgenden Schritten:

1. Rufen Sie für das entsprechende Gerät den Setup-Assistenen auf.
2. Wählen Sie den Setup-Assistenten zur Konfiguration des Content Filters.



3. Wählen Sie eines der vordefinierten Sicherheitsprofile (Basis-Profil, Firmen-Profil, Jugendschutz-Profil):

   - Basis-Profil: Diese Profil sperrt im Wesentlichen den Zugang zu den Kategorien Pornografie, illegale, gewalttätige oder diskriminierende Inhalte, Drogen, SPAM und Phishing
   - Firmen-Profil: Über die Einstellungen des Basis-Profils hinaus sperrt dieses Profil zusätzlich die Kategorien Einkaufen, Jobsuche, Spiele, Musik, Radio und bestimmte Kommunikationsdienste wie Chat.
   - Jugendschutz-Profil: Über die Einstellungen des Basis-Profils hinaus gelten in diesem Profil verschäfte Sperren für Nacktheit oder Waffen/ Militär.

   Falls die Firewall ausgeschaltet ist, schaltet der Assistent die Firewall ein. Dann prüft der Assistent, ob die Firewall-Regel für den Content-Filter richtig eingestellt ist und korrigiert diese, sofern nötig. Mit diesen Schritten haben Sie den Content-Filter aktiviert, es gelten immer die Standardeinstellungen für alle Stationen im Netzwerk mit dem ausgewählten Content-Filter-Profil und den noch leeren Black- und Whitelists. Passen Sie diese Einstellungen ggf. an Ihre Bedürfnisse an.

2.4 Die Standardeinstellungen im LANCOM Content-Filter

In der Standardeinstellung sind im LANCOM Content-Filter folgende Elemente angelegt:

- Eine Firewall-Regel
- Drei Firewall-Aktions-Objekte

- Drei Content-Filter-Profile
- Zwei Zeitrahmen
- Eine Blacklist
- Eine Whitelist
- Drei Kategorieprofile

Firewall-Regel

Die voreingestellte Firewall-Regel hat den Namen CONTENT-FILTER und verwendet das Aktionsobjekt CONTENT-FILTER-BASIC.

Wenn der LANCOM Content-Filter in ein bereits konfiguriertes Gerät eingespielt wird, wird die Firewall-Regel nicht automatisch angelegt, sondern muss manuell hinzugefügt werden. Diese Firewall-Regel muss dann eines der vordefinierten Aktions-Objekte für den Content-Filter nutzen.

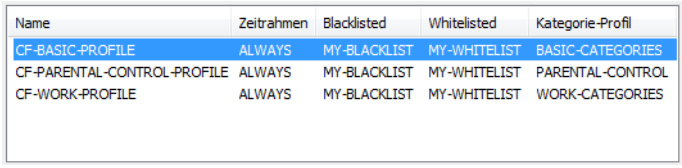
Firewall-Aktions-Objekte

Es existieren drei Firewall-Aktions-Objekte: CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK und CONTENT-FILTER-PARENTAL-CONTROL. Diese Aktionsobjekte greifen auf die entsprechenden Content-Filter-Profile zurück.

Content-Filter-Profile

Es existieren drei Content-Filter-Profile. Alle Content-Filter-Profile nutzen den zeitrahmen ALWAYS, die Blacklist MY-BLACKLIST und die Whitelist MY-WHITELIST. Jedes Content-Filter-Profil nutzt eines der vordefinierten Kategorie-Profile:

- CF-BASIC-PROFILE: Dieses Content-Filter Profil verfügt nur über geringe Einschränkungen und nutzt das Kategorie-Profil BASIC-CATEGORIES.
- CF-PARENTAL-CONTROL-PROFILE: Mit diesem Content-Filter-Profil können Minderjährige (Auszubildende) vor ungeeigneten Internetinhalten geschützt werden, es nutzt das Kategorie-Profil PARENTAL-CONTROL.
- CF-WORK-PROFILE: Dieses Content-Filter-Profil ist für den Einsatz in Unternehmen gedacht und sperrt z.B. die Kategorien Jobsuche oder Chat, es nutzt das Kategorie-Profil WORK-CATEGORIES.



Name	Zeitrahmen	Blacklisted	Whitelisted	Kategorie-Profil
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

Zeitrahmen

Es gibt zwei definierte Zeitrahmen:

- ALWAYS: 00.00-23.59 Uhr
- NEVER: 00.00-0.00 Uhr

Blacklist

Die voreingestellte Blacklist hat den Namen "MY-BLACKLIST" und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung verboten werden sollen.

Whitelist

Die voreingestellte Whitelist hat den Namen "MY-WHITELIST"und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung erlaubt werden sollen.

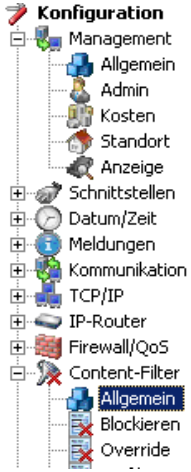
Kategorieprofile

Es existieren drei Kategorieprofie: BASIC-CATEGORIES, WORK-CATEGORIES und PARENTAL-CONTROL. Das Kategorie-Profil enthält die Angaben darüber, welche Kategorien erlaubt und verboten sind und für welche ein sogenannter Override aktiviert ist.

DE

3 Erweiterte Konfiguration des LANCOM Content Filters mit LANconfig

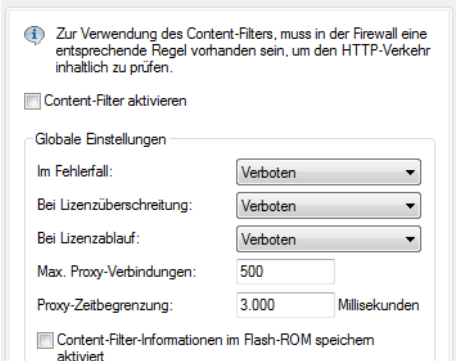
Zur Konfiguration des Content-Filter finden Sie in LANconfig ein spezielles Menü:



Der Betrieb des LANCOM Content-Filter kann durch die Datenschutzrichtlinien in Ihrem Land oder Betriebsvereinbarungen in Ihrem Unternehmen eingeschränkt sein. Bitte prüfen Sie vor Inbetriebnahme die geltenen Regelungen.

3.1 Allgemeine Einstellungen

Die globalen Einstellungen des LANCOM Content Filters nehmen Sie hier vor:



LANconfig: Content-Filter ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

- **Content-Filter aktivieren**

  Hier können Sie den LANCOM Content Filter aktivieren.

- **Im Fehlerfall:**

  Hier können Sie bestimmen, was bei einem Fehler passieren soll. Kann der Bewertungsserver beispielsweise nicht kontaktiert werden, kann der Benutzer in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

  Mögliche Werte:

  - verboten, erlaubt

  Default:

  - verboten

- **Bei Lizenzüberschreitung:**

  Hier können Sie bestimmen, was bei Überschreitung der lizensierten Benutzeranzahl passieren soll. Die Benutzer werden über die IP-Adresse identifiziert. Das heißt, dass die IP-Adressen, die eine Verbindung durch den LANCOM Content Filter aufbauen, gezählt werden. Baut z.B. bei einer 10er Option ein elfter Benutzer eine Verbindung auf, findet keine Prüfung mehr durch den LANCOM Content Filter statt. Der Benutzer, für den keine Lizenz mehr zur Verfügung steht, kann in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

  Mögliche Werte:

- verboten, erlaubt

Default:

- verboten

Die Benutzer des Content-Filters werden automatisch aus der Benutzerliste entfernt, wenn von dieser IP-Adresse seit 24 Stunden keine Verbindung durch den Content-Filter mehr aufgebaut wurde.

- **Bei Lizenzablauf:**

  Die Lizenz zur Nutzung des LANCOM Content Filters gilt für einen bestimmten Zeitraum. Sie werden 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz an die auslaufende Lizenz erinnert (an die E-Mail-adresse, die konfiguriert ist unter LANconfig: Meldungen ▶ Allgemein).

  Hier können Sie bestimmen, was bei Ablauf der Lizenz passieren soll (blockieren oder ungeprüft durchlassen). Der Benutzer kann in Folge dieser Einstellung nach Ablauf der für ihn verwendeten Lizenz entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

  Mögliche Werte:

  - verboten, erlaubt

  Default:

  - verboten

- **Max. Proxy-Verbindungen**

  Stellen Sie hier die Anzahl der Proxy-Verbindungen ein, die maximal gleichzeitig aufgebaut werden dürfen. Die Last kann somit auf dem System eingeschränkt werden. Wenn die hier eingestellte maximale Verbindungszahl erreicht wird, wird die Aktion verwendet, die bei den Ereignissen für die Proxy-Begrenzung eingestellt ist.

  Mögliche Werte:

  - 0 bis 999999 Verbindungen

  Default:

  - geräteabhängig

- **Proxy-Zeitbegrenzung**

  Die Prüfung der aufgerufenen URL kann zeitlich begrenzt werden. Wenn die hier eingestellte Zeit bei der Prüfung einer URL erreicht wird, wird die Aktion verwendet, die bei den Ereignissenfür den Fehlerfall eingestellt ist.

  Mögliche Werte:

- max. 9999 Millisekunden

Default:

- 3000 Millisekunden

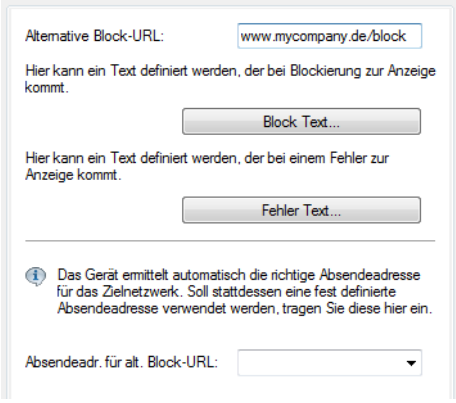
Besondere Werte:

- Der Wert 0 steht für keine Zeitbegrenzung. Werte kleiner als 100 Millisekunden sind nicht sinnvoll.

DE

3.2 Einstellungen für das Blockieren

Die Einstellungen für das Blockieren von Webseiten nehmen Sie hier vor:



LANconfig: Content-Filter ▶ Blockieren

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

- **Alternative Block-URL:**

  Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Blockierens wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z.B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen HTML-Tags wie im Blocktext verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

  Mögliche Werte:

  - gültige URL-Adresse

Default:

- leer

- **Absendeadr. für alt. Block-URL:**

  Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z.B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

  Mögliche Werte:

  - Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
  - "INT" für die Adresse des ersten Intranets
  - "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen)
  - LB0 ... LBF für die 16 Loopback-Adressen
  - GUEST
  - Beliebige IP-Adresse in der Form x.x.x.x

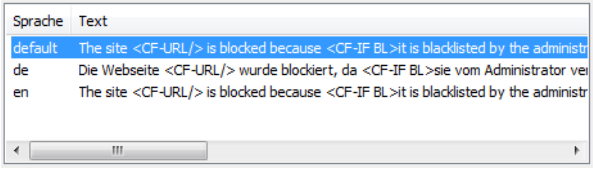
  Default:

  - leer

Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

3.2.1 Block-Text

Hier können Sie einen Text definieren, der bei Blockierung angezeigt wird. Für unterschiedliche Sprachen kann jeweils ein eigener Blocktext definiert wird. Die Auswahl des verwendeten Blocktextes wird anhand des übermittelten Spracheinstellung des Browsers (User Agents) vorgenommen.



Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z.B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Country-Code muss genau der Spracheinstellung des Browsers entsprechen, z.B. muss für Deutsch "de-DE" eingegeben werden (es reicht nicht "de"). Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

- 10 alphanumerische Zeichen

Default:

- leer

Text

Geben Sie hier den Text ein, der als Blocktext für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Blocktext auch spezielle Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z.B. Verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für die verbotene URL
- <CF-CATEGORIES/> für die Liste der Kategorien aufgrund der die Webseite verboten wurde
- <CF-PROFILE/> für den Profilnamen
- <CF-OVERRIDEURL/> für die URL zum Freischalten des Overrides (diese kann in ein einfaches <a>-Tag oder einen Button eingebaut werden)
- <CF-LINK/> fügt einen Link zum Freischalten des Overrides ein
- <CF-BUTTON/> für einen Button zum Freischalten des Overrides

Zum Ein- und Ausblenden von Teilen des Html-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute sind:

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- CATEGORY: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
- ERR: wenn ein Fehler aufgetreten ist.

  Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Tag nur sinnvoll, wenn Sie eine alternative Block-URL konfiguriert haben.
- OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z.B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Blocktext nur maximal 254 Zeichen lang sein darf.

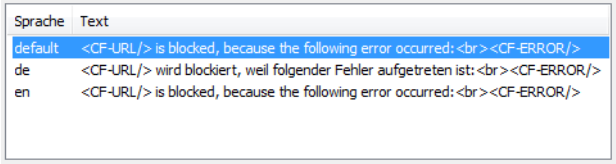
- Beispiel:

  <CF-URL/> wird wegen der Kategorien <CF-CA/> verboten.
Ihr Contentfilterprofil ist <CF-PR/>.
<CF-IF OVERRIDEOK>
<CF-BU/></CF-IF>

Die hier beschriebenen Tags können auch in externen HTML-Seiten (alternative Block-URL) verwendet werden.

3.2.2 Fehler-Text

Hier können Sie einen Text definieren, der bei einem Fehler zur Anzeige kommt.



- **Sprache**

  Hier haben Sie die gleichen Einstellungsmöglichkeiten wie unter 'Sprache' →Seite 23 beschrieben.

- **Text**

  Geben Sie hier den Text ein, der als Fehlertext für diese Sprache verwendet werden soll.

  Mögliche Werte:

  - 254 alphanumerische Zeichen

  Default:

  - leer

  Besondere Werte:

  Sie können für den Fehlertext auch HTML-Tags verwenden.

  Für die einzusetzenden Werte können Sie folgende Empty-Element-Tags verwenden:

  - <CF-URL/> für die verbotene URL
  - <CF-PROFILE/> für den Profilnamen
  - <CF-ERROR/> für die Fehlermeldung
  - Beispiel:

    <CF-URL/> wird verboten, weil ein Fehler aufgetreten ist:
<CF-ERROR/>

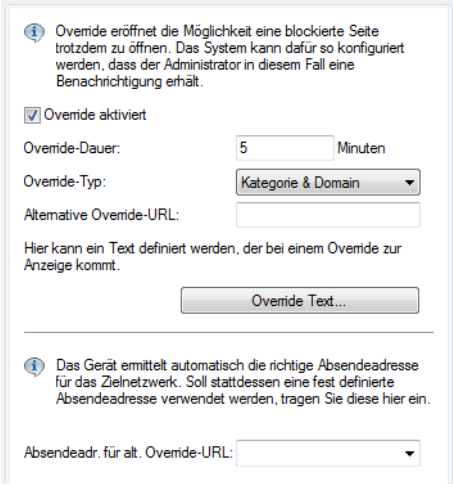
3.3 Override-Einstellungen

Die Override-Funktion ermöglicht eine Webseite zu öffnen, obwohl sie zu einer verbotenen Kategorie gehört. Wenn die verbotene Seite geöffnet werden soll, muss der Benutzer dies mit einem Klick auf den Override-Button

bestätigen. Sie können die Konfiguration so einstellen, dass der Administrator bei Klick auf den Override-Button eine Benachrichtigung erhält (LANconfig: Content-Filter ▶ Optionen).

Durch den Klick auf den Override-Button schaltet der Benutzer, wenn der Override-Typ "Kategorie" aktiviert ist, **alle** Kategorien frei, zu denen die aufgerufene URL gehört. Auf der zunächst angezeigten Blockseite wird nur eine Kategorie angezeigt, aufgrund derer der Zugriff auf die URL gesperrt werden soll. Nach dem Klick auf den Override-Button werden alle freigeschalteten Kategorien angezeigt. Wenn der Override-Typ "Domain" aktiviert ist wird die Domain freigeschaltet.

Die Einstellungen für die Override-Funktion finden Sie hier:



LANconfig: Content-Filter ▶ Override

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

- **Override aktiviert**

  Hier können Sie die Override-Funktion aktivieren und weitere Einstellungen für diese Funktion vornehmen.

- **Override-Dauer:**

  Der Override kann hier zeitlich begrenzt werden. Nach Ablauf der Zeitspanne wird jedes Betreten der gleichen Domain und/oder Kategorie wie-

der verboten. Mit einem erneuten Klick auf den Override-Button kann die Seite wieder für die Override-Dauer betreten werden, der Administrator erhält je nach Einstellung eine erneute Benachrichtigung.

Mögliche Werte:

- 1-1440 (Minuten)

Default:

- 5 (Minuten)

- **Override-Typ:**

  Hier können Sie den Override-Typ einstellen, für den der Override gelten soll. Er kann für die Domain oder die Kategorie der zu blockierenden Seite oder für beides erlaubt werden.

  Mögliche Werte:

  - Kategorie: Während der Override-Dauer sind alle URLs erlaubt, die unter die angezeigten Kategorien fallen (zuzüglich derer, die auch ohne den Override schon erlaubt gewesen wären).
  - Domain: Während der Override-Dauer sind alle URLs unter der besuchten Domain erlaubt, egal zu welchen Kategorien sie gehören.
  - Kategorie und Domain: Während der Override-Dauer sind alle URLs erlaubt, die sowohl zu dieser Domain als auch zu den freigeschalteten Kategorien gehören. Dies ist die stärkste Einschränkung.

  Default:

  - Kategorie und Domain

- **Alternative Override-URL:**

  Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Override wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z.B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen Tags wie im Override-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

  Mögliche Werte:

  - gültige URL-Adresse

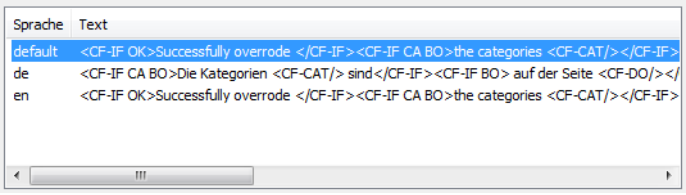
  Default:

  - leer

- **Override-Absende-IP-Adresse:**
  Hier finden Sie die gleichen Einstellungen wie unter 'Absendeadr. für alt. Block-URL:' →Seite 22.

3.3.1 Override Text

Hier können Sie einen Text definieren, der als Bestätigung für den Benutzer bei einem Override angezeigt wird.



- **Sprache**
  Hier haben Sie die gleichen Einstellungen wie unter 'Sprache' →Seite 23 beschrieben.

- **Text**
  Geben Sie hier den Text ein, der als Override Text für diese Sprache verwendet werden soll.

  Mögliche Werte:

  - 254 alphanumerische Zeichen

  Default:

  - leer

  Besondere Werte:

  Sie können für den Blocktext auch HTML-Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z.B. Verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

  Für die einzusetzenden Werte können Sie folgende Tags verwenden:

  - <CF-URL/> für die ursprünglich verbotene URL, die jetzt aber freigeschaltet ist
  - <CF-CATEGORIES/> für die Liste der Kategorien, die durch diesen Override freigeschaltet sind (außer bei Domain-Override).
  - <CF-BUTTON/> zeigt einen Override-Button, der auf die ursprünglich aufgerufene URL weiterleitet.

- <CF-LINK/> zeigt einen Override-Link an, der auf die ursprünglich aufgerufene URL weiterleitet.
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain der freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-ERROR/> erzeugt eine Fehlermeldung, falls der Override fehlschlägt.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.

Zum Ein- und Ausblenden von Teilen des Html-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute können sein:

- CATEGORY wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- DOMAIN wenn der Override-Typ "Domain" ist und der Override erfolgreich war
- BOTH wenn der Override-Typ "Kategorie und Domain" ist und der Override erfolgreich war
- ERROR falls der Override fehlgeschlagen ist
- OK falls entweder CATEGORY oder DOMAIN oder BOTH zutreffend sind

Werden in einem Tag mehrere Attribute angegeben, dann sollte der Bereich eingeblendet werden, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z.B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Text nur maximal 254 Zeichen lang sein darf.

- Beispiel:

  <CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> in der Domain <CF-DO/></CF-IF><CF-IF DO>Die Domain <CF-DO/> ist</CF-IF><CF-IF OK> für <CF-DU/> Minuten freigeschaltet.
<CF-LI/></CF-IF><CF-IF ERR>Override-Fehler:
<CF-ERR/></CF-IF>

3.4 Profile des LANCOM Content Filters

Hier können Sie Content-Filter-Profile erstellen, die zur Überprüfung von Webseiten auf nicht zugelassene Inhalte genutzt werden. Ein Content-Filter-Profil hat immer einen Namen und ordnet verschiedenen Zeitabschnitten das

jeweils gewünschte Kategorieprofil sowie optional eine Black- und eine Whitelist zu.

Um verschiedene Zeiträume unterschiedlich zu definieren, werden mehrere Content-Filter-Profileinträge mit dem gleichen Namen angelegt. Das Content-Filter-Profil besteht dann aus der Summe aller Einträge mit dem gleichen Namen.

Das Content-Filter-Profil wird über die Firewall angesprochen.

Bitte beachten Sie, dass Sie zur Nutzung der Profile im LANCOM Content Filters entsprechende Einstellungen in der Firewall vornehmen müssen.

3.4.1 Profile

Die Einstellungen für die Profile finden Sie hier:

LANconfig: Content-Filter ▶ Profile ▶ Profile

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Profile

- **Name**

  Hier muss der Name des Profils angegeben werden, über das es in der Firewall referenziert wird.

  Mögliche Werte:

  - Name eines Profils

  Default:

  - leer

Zeitrahmen

Wählen Sie den Zeitrahmen für das folgende Kategorieprofil und optional die Blacklist und die Whitelist. Voreingestellt sind die Zeitrahmen "Always" und "Never". Weitere Zeitrahmen können Sie konfigurieren unter:

LANconfig: Datum/Zeit ▶ Allgemein ▶ Zeitrahmen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zeit ▶ Zeitrahmen

Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben.

Mögliche Werte:

- Always
- Never
- Name eines Zeitrahmenprofils

Default:

- leer

Wenn sich bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil die Zeitrahmen überlappen, werden in diesem Zeitraum alle Seiten gesperrt, die durch einen der aktiven Einträge erfasst werden. Bleibt bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil ein Zeitraum undefiniert, ist in diesem Zeitraum der ungeprüfte Zugriff auf alle Webseiten möglich.

Blacklisted

Name des Blacklist-Profils das für dieses Content-Filter-Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Blacklist-Tabelle ausgewählt werden.

Mögliche Werte:

- Name eines Blacklist-Profils
- Neuer Name

Default:

- leer

Whitelisted

Name des WhiteList-Profils das für dieses Content-Filter-Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Whitelist-Tabelle ausgewählt werden.

Mögliche Werte:

- Name eines Whitelist-Profils
- Neuer Name

Default:

- leer

Kategorie-Profil

Name des Kategorie-Profils das für dieses Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Kategorietabelle ausgewählt werden.

Mögliche Werte:

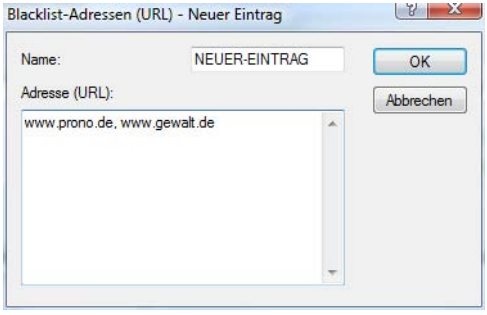
- Name eines Kategorie-Profils
- Neuer Name

Default:

- leer

3.4.2 Blacklist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die anschließend verboten werden sollen.



LANconfig: Content-Filter ▶ Profile ▶ Blacklist-Adressen (URL)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Blacklists

Name

Hier muss der Name der Blacklist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name einer Blacklist

Default:

- leer

- **Adresse (URL)**

  Hier werden die URLs eingetragen, die über diese Blacklist verboten werden sollen.

  Mögliche Werte:

  - gültige URL-Adresse

  Es können auch folgende Wildcards zum Einsatz kommen:

  - * für mehrere beliebige Zeichen (z.B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.eu, www.lancom.es etc.)
  - ? für ein beliebiges Zeichen (z.B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)

Bitte geben Sie die URL **ohne** führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z.B. www.mycompany.de/ . Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de* .

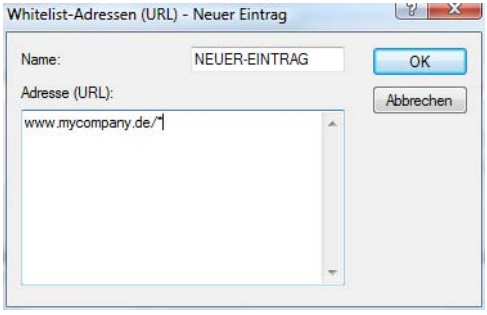
Einzelne URLs werden mit Leerzeichen getrennt.

Default:

- leer

3.4.3 Whitelist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die gezielt erlaubt werden sollen.



LANconfig: Content-Filter ▶ Profile ▶ Whitelist-Adressen (URL)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Whitelists

- **Name**

  Hier muss der Name der Whitelist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

  Mögliche Werte:

  - Name einer Whitelist

  Default:

  - leer

- **Adressen (URL)**

  Hier können Sie Webseiten konfigurieren, die lokal geprüft und anschließend akzeptiert werden sollen.

  Mögliche Werte:

  - gültige URL-Adresse

  Es können auch folgende Wildcards zum Einsatz kommen:

  - * für mehrere beliebige Zeichen (z.B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.eu, www.lancom.es etc.)
  - ? für ein beliebiges Zeichen (z.B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)

  Bitte geben Sie die URL **ohne** führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z.B. www.mycompany.de/ . Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de* .

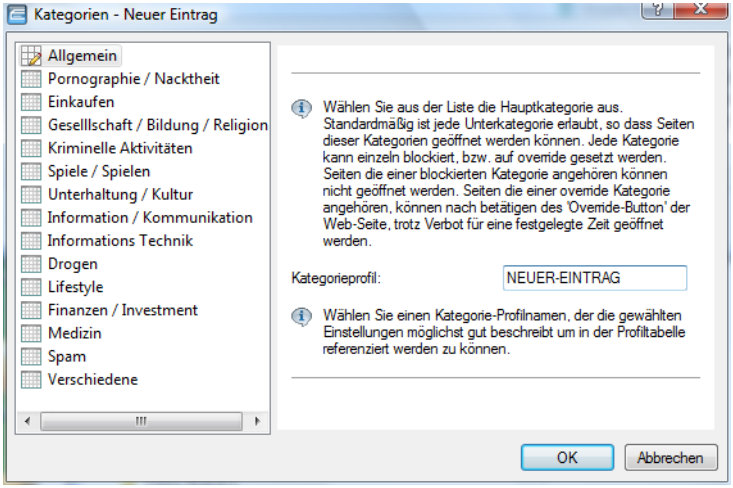
  Einzelne URLs werden mit Leerzeichen getrennt.

  Default:

  - leer

3.4.4 Kategorien

Hier erstellen Sie ein Kategorieprofil und legen fest, welche Kategorien bzw. Gruppen bei der Bewertung der Webseiten berücksichtigt werden. Für jede Gruppe können Sie die einzelnen Kategorien erlauben, verbieten oder die Override-Funktion aktivieren.



LANconfig: Content-Filter ▶ Profile ▶ Kategorien

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Kategorieprofile

- **Kategorieprofil**

  Hier wird der Name der Kategorieprofils angegeben, über den sie im Content-Filter-Profil referenziert wird.

  Mögliche Werte:

  - Name eines Kategorieprofils

  Default:

  - leer

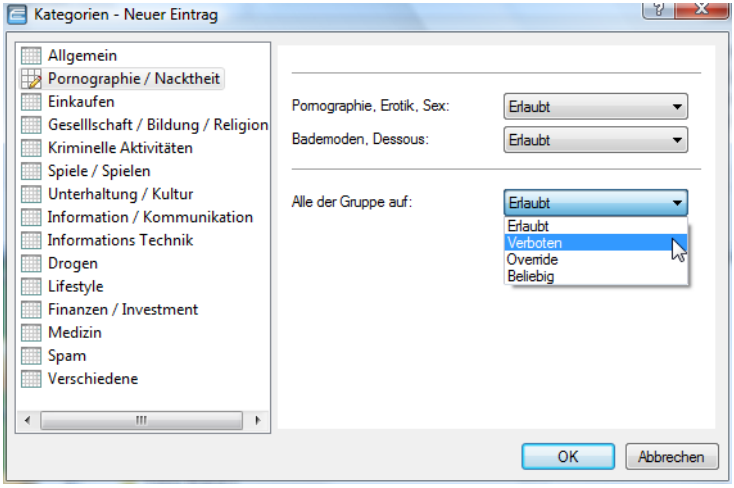
- **Kategorieeinstellungen**

  Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

  Folgende Hauptkategorien können konfiguriert werden:

  - Pornographie/ Nacktheit
  - Einkaufen
  - Gesellschaft/ Bildung/ Religion
  - Kriminelle Aktivitäten
  - Spiele/ Spielen

- Unterhaltung/ Kultur
- Information/ Kommunikation
- Informationstechnik
- Drogen
- Lifestyle
- Finanzen/ Investement
- Medizin
- Spam
- Verschiedene



Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

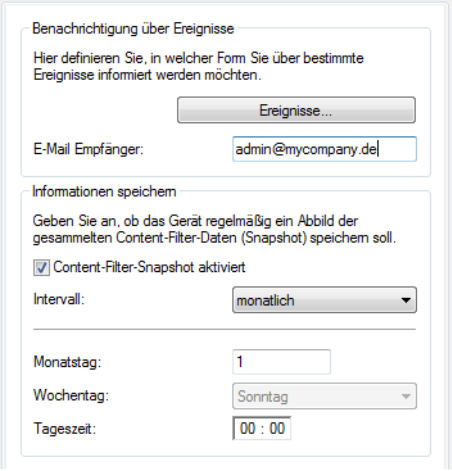
- Erlaubt, Verboten, Override

Default:

- Erlaubt

3.5 Optionen des LANCOM Content Filters

Hier können Sie einstellen, ob Sie über Ereignisse benachrichtigt werden und an wo die Informationen des LANCOM Content Filters gespeichert werden sollen.



LANconfig: Content-Filter ▶ Optionen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

- **Ereignisse:**

  Hier definieren Sie, in welcher Form Sie über bestimmte Ereignisse informiert werden. Die Benachrichtigung kann erfolgen durch E-Mail, SNMP oder SYSLOG. Für verschiedene Ereignisse kann separat definiert werden, über welchen Weg Meldungen ausgegeben werden sollen.

  Fehler:

  - Bei SYSLOG: Quelle "System", Priorität "Alarm".
  - Default: Benachrichtigung SNMP

  Lizenzablauf:

  - Bei SYSLOG: Quelle "Verwaltung", Priorität "Alarm".
  - Default: Benachrichtigung SNMP

  Lizenz überschritten:

  - Bei SYSLOG: Quelle "Verwaltung", Priorität "Alarm".
  - Default: Benachrichtigung SNMP

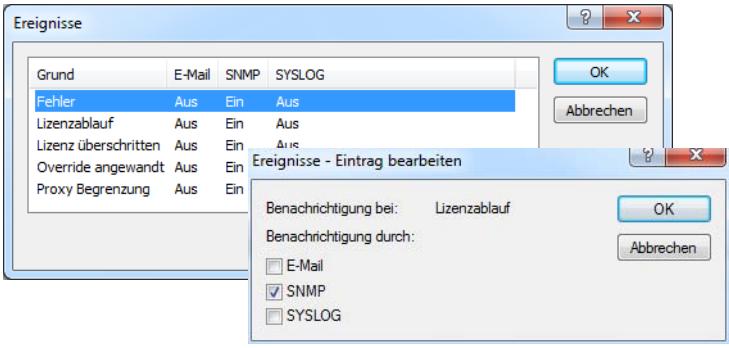
  Override angewandt:

  - Bei SYSLOG: Quelle "Router", Priorität "Alarm".
  - Default: Benachrichtigung SNMP

  Proxy-Begrenzung:

DE

- Bei SYSLOG: Quelle “Router”, Priorität “Info”.
- Default: Benachrichtigung SNMP



E-Mail Empfänger:

Um die E-Mail Benachrichtigungsfunktion zu nutzen, muss ein SMTP-Client entsprechend konfiguriert sein. Sie können den Client in diesem Gerät dazu verwenden oder einen anderen Ihrer Wahl.

Wenn kein E-Mail Empfänger angegeben wird, dann wird keine E-Mail verschickt.

Content-Filter-Snapshot

Hier können Sie den Content-Filter-Snapshot aktivieren und bestimmen wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

Intervall

Wählen Sie hier, ob der SnapShot monatlich, wöchentlich oder täglich angefertigt werden soll.

Mögliche Werte:

- monatlich
- wöchentlich
- täglich

Default:

- monatlich

- **Monatstag:**

  Ist eine monatliche Ausführung des SnapShot gewünscht, wählen Sie hier den Tag an dem der SnapShot angefertigt werden soll.

  Mögliche Werte:

  - max. 2 Zeichen

  Default:

  - 1

Wählen Sie als Monatstag sinnvollerweise eine Zahl zwischen 1 und 28, damit der Tag in jedem Monat vorkommt.

- **Wochentag:**

  Ist eine wöchentliche Ausführung des SnapShot gewünscht, selektieren Sie hier den Wochentag, an dem der SnapShot angefertigt werden soll.

  Mögliche Werte:

  - Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

  Default:

  - Montag

- **Tageszeit:**

  Ist eine tägliche Ausführung des SnapShot gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein.

  Mögliche Werte:

  - max. 5 Zeichen, Format HH:MM

  Default:

  - 00:00

3.6 Zusätzliche Einstellungen für den LANCOM Content Filter

3.6.1 Firewall-Einstellungen für den Content-Filter

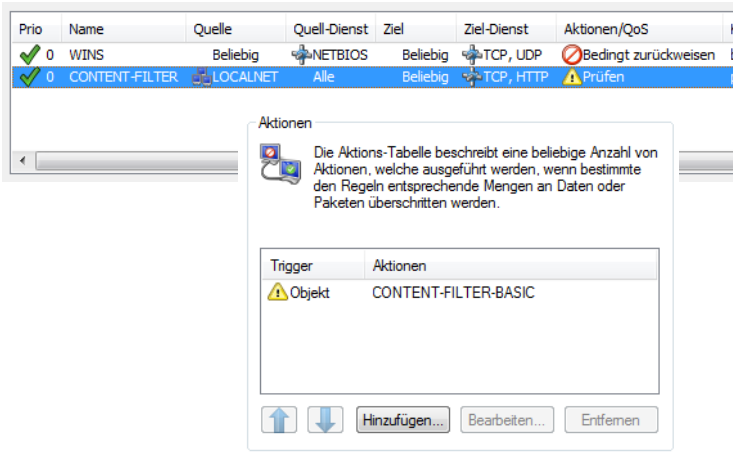
Die Firewall muss aktiviert sein, damit der LANCOM Content Filter arbeiten kann. Sie aktivieren die Firewall unter:

LANconfig: Firewall/QoS ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ Firewall

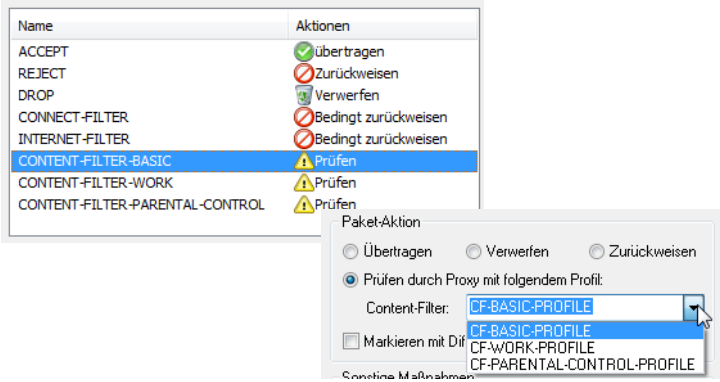
DE

In der Default-Einstellung finden Sie die Firewall-Regel CONTENT-FILTER, die auf das Aktionsobjekt CONTENT-FILTER-BASIC zurückgreift:



Die Firewall-Regel sollte auf den Zieldienst "http" beschränkt werden, damit nur ausgehende HTTP-Verbindungen erfasst werden. Ohne diese Einschränkung werden alle Pakete über den Contentfilter geprüft, was zu einer Beeinträchtigung der Perfomance im Gerät führt.

Eine Firewall-Regel für den Content-Filter muss ein spezielles Aktionsobjekt verwenden, das über die Paket-Aktionen die Daten mit einem Content-Filter-Profil prüft. In der Default-Einstellung finden Sie die Aktionsobjekte CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK und CONTENT-FILTER-PARENTAL-CONTROL, die auf jeweils passende Content-Filter-Profile zurückgreifen:

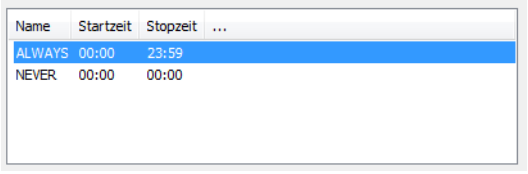


Beispiel: Beim Öffnen einer Webseite durchlaufen die Datenpakte die Firewall und werden von der Regel CONTENT-FILTER erfasst. Das Aktionsobjekt CONTENT-FILTER-BASIC prüft die Datenpakete mit dem Content-Filter-Profil CONTENT-FILTER-BASIC.

3.6.2 Zeitrahmen

Zeitrahmen werden verwendet, um die Gültigkeitsdauer von Content-Filter-Profilen zu definieren. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Dabei sollten sich die Zeitrahmen unterschiedlicher Zeilen ergänzen, d.h. wenn Sie eine ARBEITSZEIT festlegen, wollen Sie wahrscheinlich auch einen Zeitrahmen FREIZEIT festlegen, der die Zeit außerhalb der Arbeitszeit umfasst.

Voreingestellt sind die Zeitrahmen “ALWAYS” und “NEVER”. Weitere Zeitrahmen können Sie konfigurieren unter:



LANconfig: Datum/Zeit ▶ Allgemein ▶ Zeitrahmen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zeit ▶ Zeitrahmen

- **Name**

  Hier muss der Name des Zeitrahmens angegeben werden, über den er im Content-Filter-Profil referenziert wird.

DE

Mögliche Werte:

- Name eines Zeitrahmens

Default:

- leer

Startzeit

Hier kann die Startzeit (Tageszeit) angegeben werden, ab der das gewählte Profil gelten soll.

Mögliche Werte:

- max. 5 Zeichen, Format HH:MM

Default:

- 00:00

Endzeit

Hier kann die Endzeit (Tageszeit) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein soll.

Mögliche Werte:

- max. 5 Zeichen, Format HH:MM

Default:

- 23:59

Wochentage

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Default:

- Aktiviert für Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren:

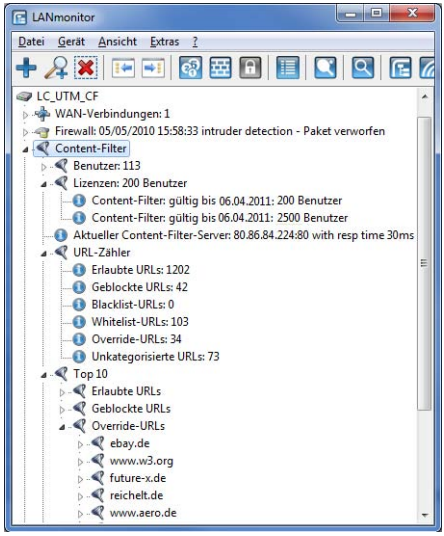
Name	Startzeit	Stopzeit	...
ALWAYS	00:00	23:59	
FREIZEIT	00:00	07:00	
FREIZEIT	12:01	13:00	
FREIZEIT	17:01	23:59	
NEVER	00:00	00:00	

DE

4 Statusmeldungen

4.1 LANmonitor

Mit dem LANmonitor können Sie die wichtigsten Statusmeldungen des LANCOM Content-Filters auf einen Blick einsehen.



4.1.1 Anzeigen des LANCOM Content-Filters in der Übersicht

LANmonitor zeigt die folgenden Informationen über den LANCOM Content-Filter:

- IP-Adressen und MAC-Adressen der Benutzer
- Informationen über die Lizenz für den LANCOM Content-Filter
- Informationen über den aktuell verwendeten Content-Filter-Server
  - Benutzt seit: Zeitpunkt, ab dem der angegebene Rating-Server verwendet wurde.
  - Erste Antwortzeit: Dauer für die erste Antwort des Rating-Servers.
  - Verarbeitete URLs: Anzahl der URLs, die geprüft wurden.
  - Verarbeitungstimeouts: Anzahl der URL-Prüfungen, die nicht innerhalb des eingestellten Timeouts beantwortet wurden.
  - Minimale Verarbeitungszeit: Minimale Dauer der URL-Prüfungen.

DE

- Maximale Verarbeitungszeit: Maximale Dauer der URL-Prüfungen, sofern diese kleiner ist als der Timeout-Wert.
- Durchschnittliche Verarbeitungszeit: Durchschnittliche Dauer der URL-Prüfungen.
- Durchschnittliche Verarbeitungszeit (letzte 5 Minuten): Durchschnittliche Dauer der URL-Prüfungen in den letzten 5 Minuten.
- Ratingserveranfragen: Anzahl der URL-Anfragen, die beim Ratingserver geprüft wurden.
- Ratingserver-Timeouts: Anzahl der URL-Prüfungen beim Ratingserver, die nicht innerhalb des eingestellten Timeouts beantwortet wurden.
- Minimale Ratingserver-Antwortzeit: Minimale Bearbeitungsdauer der Anfragen beim Ratingserver.
- Maximale Ratingserver-Antwortzeit: Maximale Bearbeitungsdauer der Anfragen beim Ratingserver, sofern diese kleiner ist als der Timeout-Wert.
- Durchschnittliche Ratingserver-Antwortzeit: Durchschnittliche Bearbeitungsdauer der Anfragen beim Ratingserver
- Durchschnittliche Ratingserver-Antwortzeit (letzte 5 Minuten): Durchschnittliche Bearbeitungsdauer der Anfragen beim Ratingserver in den letzten 5 Minuten.

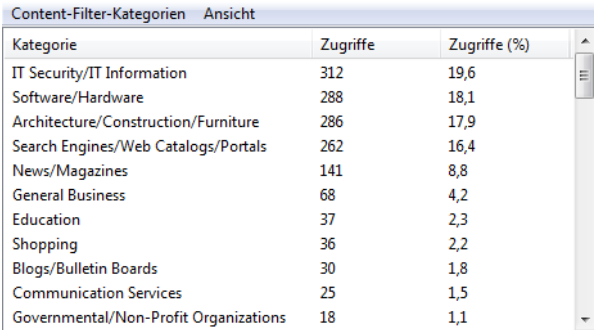
- URL-Zähler mit den erlaubten URLs, geblockten URLs, Black- und Whitelist-URLs, Override-URLs und den unkategorisierten URLs. (Es werden nur URLs ohne Pfad gezählt).
- URL-Zähler für die geblockten URLs, URLs in Black- und White-Listen, URLs auf die mit Hilfe des Override zugegriffen wurde und nicht kategorisierte URLs.
- Top-10 für die erlaubten URLs, geblockten URLs und die URLs auf die mit Hilfe des Override zugegriffen wurde. Es wird die ermittelte Kategorie sowie die Anzahl der Zugriffe angegeben.
- Cache-Nutzung: Nutzung des Cache-Speichers für die Kategorisierung der URLs.
- Cache-Trefferrate: Anteil der URL-Anfragen, die vom Cache-Speicher beantwortet werden konnten.

4.1.2 Detail-Anzeigen des LANCOM Content-Filter

Über das Menü des LANCOM Content-Filter können Sie zwei weitere Fenster mit zusätzlichen Informationen öffnen. Klicken Sie dazu mit der rechten

Maustaste auf den "Content-Filter" und wählen Sie den entsprechneden Eintrag im Kontextmenü.

Content-Filter-Kategorien anzeigen

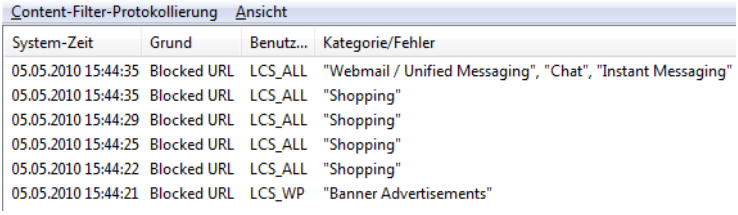


Kategorie	Zugriffe	Zugriffe (%)
IT Security/IT Information	312	19,6
Software/Hardware	288	18,1
Architecture/Construction/Furniture	286	17,9
Search Engines/Web Catalogs/Portals	262	16,4
News/Magazines	141	8,8
General Business	68	4,2
Education	37	2,3
Shopping	36	2,2
Blogs/Bulletin Boards	30	1,8
Communication Services	25	1,5
Governmental/Non-Profit Organizations	18	1,1

Dieser Dialog zeigt die Liste aller Kategorien mit der Anzahl der blockierten Zugriffe auf den Content-Filter und den prozentualen Anteil an allen Zugriffen.

Über das Menü **Content-Filter-Kategorien** können Sie die aktuell angezeigten Werte in eine Datei speichern oder gespeicherte Werte zur Anzeige im LANmonitor laden.

Content-Filter-Protokollierung anzeigen



System-Zeit	Grund	Benutz...	Kategorie/Fehler
05.05.2010 15:44:35	Blocked URL	LCS_ALL	"Webmail / Unified Messaging", "Chat", "Instant Messaging"
05.05.2010 15:44:35	Blocked URL	LCS_ALL	"Shopping"
05.05.2010 15:44:29	Blocked URL	LCS_ALL	"Shopping"
05.05.2010 15:44:25	Blocked URL	LCS_ALL	"Shopping"
05.05.2010 15:44:22	Blocked URL	LCS_ALL	"Shopping"
05.05.2010 15:44:21	Blocked URL	LCS_WP	"Banner Advertisements"

Dieser Dialog zeigt die protokollierten Detailinformationen über jeden einzelnen Zugriff auf den Content-Filter mit den folgenden Angaben:

- Systemzeit
- Grund für den Logeintrag
- Benutzer/ Profil
- Kategorie/Fehler
- aufgerufene URL

Über das Menü **Content-Filter-Protokollierung** können Sie die aktuell angezeigten Werte zurücksetzen.

4.1.3 Funktionen im LANmonitor

Mit weiteren Funktionen können Sie die Anzeigen des LANmonitor beeinflussen:

- Klicken Sie im LANmonitor mit der rechten Maustaste auf den Eintrag URL-Zähler und wählen Sie im Kontextmenü den Punkt **URL-Zähler zurücksetzen**, um die Werte in diesem Bereich auf Null zu setzen.
- Klicken Sie im LANmonitor mit der rechten Maustaste auf den Eintrag Top-10 und wählen Sie im Kontextmenü den Punkt **Top-10-Listen und Cache löschen**, um die Werte in diesem Bereich auf Null zu setzen.

4.2 WEBconfig

Über die im LANmonitor angezeigten Statusinformationen hinaus können Sie die vollständigen Statusmeldungen mit WEBconfig einsehen unter:

WEBconfig: LCOS-Menübaum ▶ Status ▶UTM ▶Content-Filter

Im Folgenden finden Sie die Beschreibungen der einzelnen Statusmeldungen:

- **Anzahl-unkategorisierter-URLs**

  Gibt die Aufrufe von Webseiten an, die keiner Kategorie zugeordnet sind.

- **Blacklist-URLs**

  Gibt die Anzahl der Webseiten, an die aufgerufen wurden und der Blacklist zugeordnet sind.

- **Erlaubte-URLs**

  Anzahl der Webseiten, die aufgerufen wurden und erlaubt sind.

- **Fehleranzahl**

  Gibt die Anzahl der Fehler an. Ein Fehler kann z.B. auftreten, wenn der Bewertungsserver nicht kontaktiert werden kann.

- **Geblockte-URLs**

  Anzahl der Webseiten, die aufgerufen wurden und verboten sind.

- **Lizenzanzahl**

  Anzahl der von Ihnen erworbenen Lizenzen. Zusätzliche Lizenzen können Sie über den Fachhandel erwerben.

- **Override-URLs**

  Anzahl der Webseiten auf die mit dem Override zugegriffen wurde. Mit der Override-Funktion können Sie einem Benutzer erlauben nach Rückfrage eine Webseite zu öffnen, obwohl sie verboten ist.

- **Whitelist-URLs**

  Gibt die Anzahl der Webseiten an, die aufgerufen wurden und der Whitelist zugeordnet sind.

- **Cache-loeschen**

  Hier haben Sie die Möglichkeit den Cache und alle drei Top-10-Listen zu löschen. Die Cache-Current-Size wird danach 0 sein, die Cache-Maximum-Size bleibt unverändert.

- **Kategorienliste-loeschen**

  Hier haben Sie die Möglichkeit die Kategorienliste und den Last-Snapshot zu löschen.

- **Logs-loeschen**

  Hier haben Sie die Möglichkeit die Log-Table und das Override-Log zu löschen.

- **Statistiken-loeschen**

  Hier haben Sie die Möglichkeit die Statistiken zu löschen. Die Zähler werden auf 0 gesetzt.

4.2.1 Benutzer

Die Benutzer-Tabelle gibt die IP-Adresse und die MAC-Adresse aller aktuellen Benutzer des Content-Filters an.

- **IP-Adresse**

  Gibt die IP-Adresse des Benutzers an.

- **MAC-Adresse**

  Gibt die MAC-Adresse des Benutzers an.

4.2.2 Kategoriestatistik

In der Kategoriestatistik sehen Sie alle Kategorien und die Anzahl der zu dieser Kategorie zugeordneten Webseiten die von einem Benutzer aufgerufen wurden.

- **Kategorie**

  Name der Kategorie.

- **Anzahl**

  Anzahl der Webseiten die dieser Kategorie zugeordnet sind.

4.2.3 Letzter-Schnappschuss

In der Liste des letzten Schnappschusses sehen Sie alle Kategorien und die Anzahl der zu dieser Kategorie zugeordneten Webseiten. Wie oft ein Schnappschuss stattfindet, können Sie konfigurieren (siehe 'Optionen des LANCOM Content Filters' →Seite 36). Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Letzter-Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

- **Kategorie**

  Name der Kategorie.

- **Anzahl**

  Anzahl der Webseiten die dieser Kategorie zugeordnet sind.

4.2.4 Log

Die Logtabelle gibt die System-Zeit des Logs, den Grund für den Log und zusätzliche Informationen über das Benutzerprofil, die Kategorie bzw. den Fehler und die URL an.

- **System-Zeit**

  Gibt den Zeitpunkt des Logs an.

- **Grund**

  Gibt den Grund für den Log an.

- **Benutzer/Profil**

  Hier steht der Name des Benutzerprofils oder die IP-Adresse des Benutzers.

- **Kategorie/Fehler**

  Wurde die Seite verboten, steht hier die Liste der Kategorien oder der Name der Blacklist, aufgrund welcher die Webseite verboten wurde.

  Wenn die Seite aufgrund eines Fehlers nicht angezeigt werden konnte, steht hier die Fehlerursache.

  Bei Lizenzüberschreitung oder -ablauf steht hier, ob die Seite gesperrt oder durchgelassen wurde.

- **URL**

  Hier steht die URL, die der Benutzer aufrufen will.

  Bei Lizenzüberschreitung oder -ablauf bleibt dieser Eintrag leer.

4.2.5 Overridelog

- **Datum/Uhrzeit**

  Gibt Datum und Uhrzeit des Overrides an.

- **Benutzer-IP**

  Gibt die IP-Adresse des Benutzers an, der den Override ausgeführt hat.

- **Benutzer-MAC**

  Gibt die MAC-Adresse des Benutzers an, der den Override ausgeführt hat.

- **Ziel-URL**

  Gibt die Webeseite an, für die der Override ausgeführt wurde.

4.2.6 Cache

- **Aktuelle Cachegroesse**

  Gibt die aktuelle Größe des Chaches an. Der Cache speichert Kategorisierungen von URLs, die beim Bewertungsserver angefragt werden. Es existiert ein Cache-Eintrag pro Domain. Die Cachegröße beeinflusst, wie oft beim Server angefragt werden muss.

- **Maximale-Cachegroesse**

  Hier ist die maximale Größe des Chaches angegeben.Der Cache speichert Kategorisierungen von URLs, die beim Bewertungsserver angefragt werden. Es existiert ein Cache-Eintrag pro Domain. Die Cachegröße beeinflusst, wie oft beim Server angefragt werden muss.

- **Trefferrate-in-%**

  Anteil der URL-Anfragen, die vom Cache-Speicher beantwortet werden konnten.

Top-10-erlaubter-URLs

In dieser Tabelle werden die zehn am häufigsten aufgerufenen Webseiten aus der Whitelist angegeben.

- **Host**

  Gibt den Host der Webseite an.

- **Kategorie**
  Gibt die Kategorie an, der die Webseite zugeordnet ist.
- **Anzahl**
  Anzahl der erlaubten Aufrufe dieser Webseite.

Top-10-geblockter-URLs

In dieser Tabelle werden die zehn Webseiten aus der Blacklist angegeben, auf die am häufigsten versucht wurde zuzugreifen.

- **Host**
  Gibt den Host der Webseite an.
- **Kategorie**
  Gibt die Kategorie an, der die Webseite zugeordnet ist.
- **Anzahl**
  Anzahl der versuchten Aufrufe dieser Webseite.

Top-10-Override-URLs

In dieser Tabelle werden die zehn am häufigsten mit der Override-Funktion aufgerufenen Webseiten angegeben.

- **Host**
  Gibt den Host der Webseite an.
- **Kategorie**
  Gibt die Kategorie an, der die Webseite zugeordnet ist.
- **Anzahl**
  Anzahl der Aufrufe dieser Webseite, die durch einen aktiven Override erlaubt wurden.

4.2.7 Performance

- **5Min-Pruefdauer**
  Durchschnittliche Dauer der URL-Prüfungen in den letzten 5 Minuten.
- **5Min-Serverzeit**
  Durchschnittliche Bearbeitungsdauer der Anfragen beim Ratingserver in den letzten 5 Minuten.
- **Anf-Serverzeit**
  Dauer für die erste Antwort des Rating-Servers.

- **Benutzt-seit**
  Zeitpunkt, ab dem der angegebene Rating-Server verwendet wurde.
- **Gepruefte-URLs**
  Anzahl der URLs, die geprüft wurden.
- **Max-Pruefdauer**
  Maximale Dauer der URL-Prüfungen, sofern diese kleiner ist als der Timeout-Wert.
- **Max-Serverzeit**
  Maximale Bearbeitungsdauer der Anfragen beim Ratingserver, sofern diese kleiner ist als der Timeout-Wert.
- **Min-Pruefdauer**
  Minimale Dauer der URL-Prüfungen.
- **Min-Serverzeit**
  Minimale Bearbeitungsdauer der Anfragen beim Ratingserver.
- **Mitt-Pruefdauer**
  Durchschnittliche Dauer der URL-Prüfungen.
- **Mitt-Serverzeit**
  Durchschnittliche Bearbeitungsdauer der Anfragen beim Ratingserver
- **Pruef-Timeouts**
  Anzahl der URL-Prüfungen, die nicht innerhalb des eingestellten Timeouts beantwortet wurden.
- **Ratingserver**
  Gibt den aktuellen Server an, den der Content-Filter kontaktiert und der . gemäß den von Ihnen ausgewählten Kategorien die Bewertung der Internetseiten zuverlässig und korrekt vornimmt.
- **Serveranfragen**
  Anzahl der URL-Anfragen, die beim Ratingserver geprüft wurden.
- **Server-Timeouts**
  Anzahl der URL-Prüfungen beim Ratingserver, die nicht innerhalb des eingestellten Timeouts beantwortet wurden.

Performace-Log

In dieser Tabelle werden die oben Performance-Tabelle aufgeführten Werte für jeden verwendeten Ratingserver gespeichert. So können die Performance-Werte für einen Ratingserver auch nachträglich geprüft werden.

4.2.8 Proxy-Verbindungen

In diesem Menü finden Sie Informationen über die statistischen Werte bei der Nutzung des Proxies im Content Filter.

- **Abgelehnte-Verbindungsversuche**
  Anzahl der Verbindungen, die vom Content-Filter-Proxy abgelehnt wurden.
- **Aktuelle-Verbindungen**
  Aktuelle Anzahl der aktiven Verbindungen zum Content-Filter-Proxy.
- **Durchschnittliche-Verbindungen**
  Durchschnittliche Anzahl der Verbindungen zum Content-Filter-Proxy.
- **Gesamte-Verbindungen**
  Gesamte Anzahl der Verbindungen zum Content-Filter-Proxy.
- **Max-Verbindungen**
  Maximale Anzahl der gleichzeitigen Verbindungen zum Content-Filter-Proxy.
- **Proxyverbindungs-Limit**
  Maximale Anzahl der erlaubten Verbindungen zum Content-Filter-Proxy.
- **Verbindungen-Letzte-5Min**
  Anzahl der Verbindungen zum Content-Filter-Proxy innerhald der letzten 5 Minuten.
- **Verbindungs-Statistik-gefuehrt-seit**
  Zeitpunkt, zu dem die Verbindungsstatistik gestartet wurde.

5 Tutorial: Mehrere Content-Filter-Profile nutzen

Dieses Kapitel zeigt Ihnen wie Sie mehrere Content-Filter-Profile sinnvoll nutzen können und welche Einstellungen Sie dabei berücksichtigen müssen.

Der LANCOM Content-Filter bietet Ihnen die Möglichkeit, mehrere Content-Filter-Profile zu konfigurieren. Sie können diese Option nutzen, um in Ihrem Unternehmen z.B. ein Content-Filter-Profil für Ihre Mitarbeiter anzulegen und ein weiteres Content-Filter-Profil für Ihre Auszubildenden. Besonders wenn ein Unternehmen minderjährige Auszubildenden beschäftigt, kann das nicht nur sinnvoll, sondern rechtlich notwendig sein.

Im Folgenden werden exemplarisch die Schritte beschrieben, die Sie für das Einrichten verschiedener Content-Filter-Profile z.B. für Ihre Mitarbeiter und Ihre Azubis durchführen müssen.

1. Aktivieren Sie den LANCOM Content-Filter unter:

   LANconfig: Content-Filter ▶ Allgemein

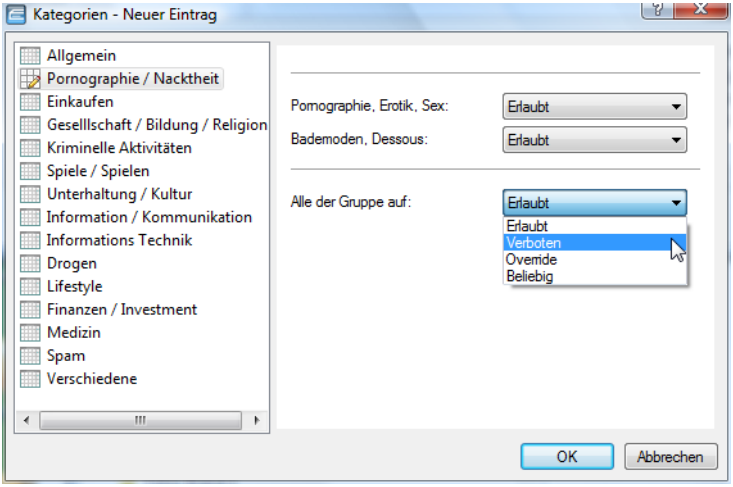
   WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Aktiv

2. Erstellen Sie Ihre Content-Filter-Profile unter:

   LANconfig: Content-Filter ▶ Profile

   WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Profile

3. Erstellen Sie unter **Kategorien** ein oder mehrere Kategorieprofile und geben Sie Ihnen einen Namen. Wenn Sie z.B. für Ihre Mitarbeiter während der Arbeitszeit andere Webseiten zulassen bzw. verbieten wollen, als in der Freizeit, dann erstellen Sie z.B. das Kategorieprofil WORK_CATEGORIES und das Kategorieprofil BASIC_CATEGORIES. Für Ihre Auszubildenden können Sie z.B. das Kategorieprofil TRAINEE_CATEGORIES erstellen. Für jedes Kategorieprofil bestimmen Sie welche Kategorien bzw. Gruppen bei der Bewertung der Webseiten berücksichtigt werden. Für jede der 14 Gruppen können Sie die einzelnen Kategorien erlauben, verbieten oder die Override-Funktion aktivieren.



4. Anschließend erstellen Sie unter **Profile** Ihre Content-Filter-Profile. Ein Content-Filter-Profil ordnet unterschiedlichen Zeitrahmen die jeweils gültigen Kategorieprofile und optional Black- und Whitelisten zu. Das Content-Filter-Profil wird über die Firewall angesprochen.

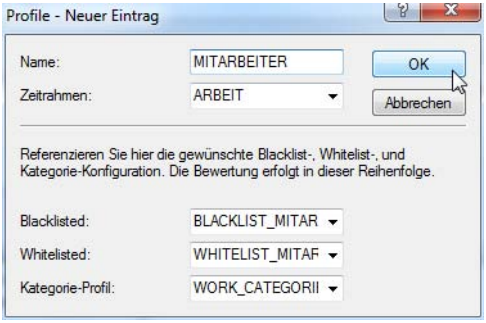
5. Geben Sie für das Content-Filter-Profil MITARBEITER den **Namen** MITARBEITER ein. Wählen Sie unter **Zeitrahmen** die Zeit in der das Kategorieprofil gelten soll, z.B. "ALWAYS". Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Dabei sollten sich die Zeitrahmen unterschiedlicher Zeilen ergänzen, d.h. wenn Sie einen Zeitrahmen ARBEIT festlegen, ist dies nur sinnvoll, wenn Sie auch einen Zeitrahmen FREIZEIT festlegen. Voreingestellt sind die Zeitrahmen "ALWAYS" und "NEVER". Weitere Zeitrahmen (z.B. jeweils einen für die Arbeitszeit und einen für die Freizeit der Mitarbeiter) können Sie konfigurieren unter:

   LANconfig: Datum/Zeit ▶ Allgemein ▶ Zeitrahmen

   WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zeit ▶ Zeitrahmen

6. Unter **Blacklisted** bzw. **Whitelisted** können Sie eine Blacklist bzw. eine Whitelist auswählen, die Sie erstellt haben, z.B. Blacklist_Mitarbeiter und Whitelist_Mitarbeiter. Unter **Kategorie-Profil** wählen Sie das Kategorie-Profil das für dieses Content-Filter-Profil im gewählten Zeitrahmen gelten soll, in diesem Beispiel MITARBEITER. Damit sind die Einstellungen für das Content-Filter-Profil MITARBEITER im Content-Filter abgeschlossen und

Sie können bei Bedarf weitere Content-Filter-Profile in der gleichen Weise anlegen.



7. Wenn Sie ein Content-Filter-Profil für Ihre Mitarbeiter und Ihre Auszubildenden angelegt haben, kann die Übersicht Ihrer Content-Filter-Profile anschließend z.B. folgendermaßen aussehen:

Name	Zeitrahmen	Blacklisted	Whitelisted	Kategorie-Profil
MITARBEITER	ARBEIT	BLACKLIST_MITARBEITER	WHITELIST_MITARBEITER	WORK_CATEGORIES
MITARBEITER	FREIZEIT	BLACKLIST_MITARBEITER	WHITELIST_MITARBEITER	BASIC_CATEGORIES
TRAINEE	ALWAYS	BLACKLIST_MITARBEITER	WHITELIST_MITARBEITER	TRAINEE_CATEGORIES

Wenn Sie verschiedene Content-Filter-Profile angelegt haben, müssen Sie die Einstellungen der Firewall anpassen (vergleiche auch 'Firewall-Einstellungen für den Content-Filter' →Seite 39).

8. Für jedes Content-Filter-Profil muss in der Firewall eine Firewall-Regel existieren. Jeder Firewall-Regeln muss ein Aktions-Objekt zugeordnet sein, welches das Content-Filter-Profil auswählt. Ein Aktions-Ojekt kann mehreren Firewall-Regeln zugeordnet werden.

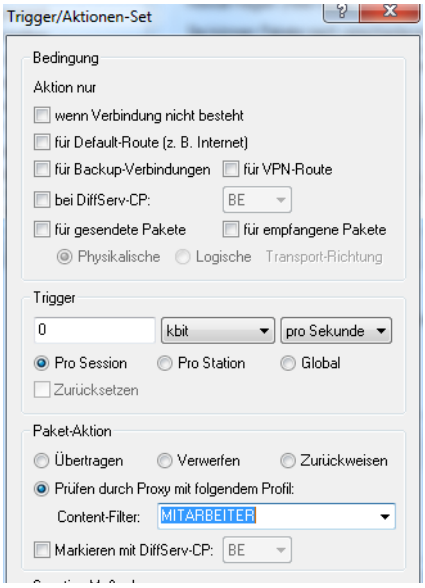
   Das Aktions-Objekt und die Firewall-Regeln finden Sie unter:

   LANconfig: Firewall/QoS ▶ Regeln

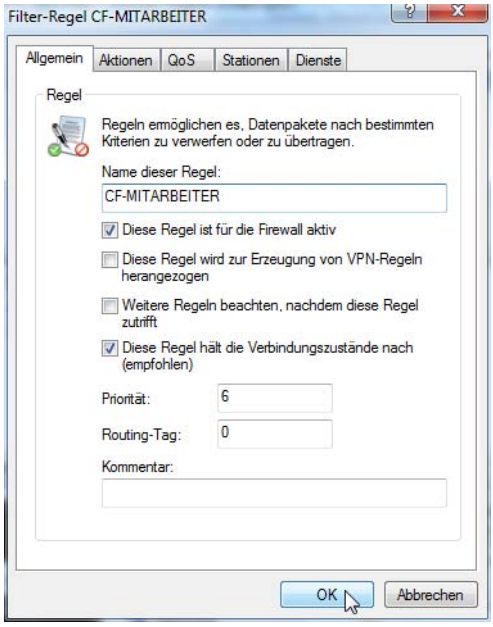
   WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ Firewall

9. Exemplarisch werden im Folgenden die Einstellungen gezeigt, die Sie z.B. für Ihr Content-Filter-Profil MITARBEITER in der Firewall vornehmen können:

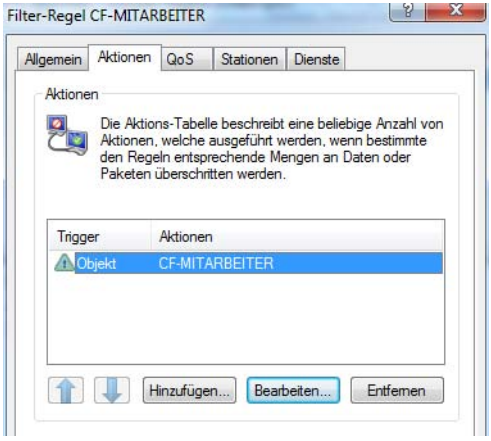
Fügen Sie unter **Aktions-Objekte** ein neues Aktionsobjekt mit dem Namen "CONTENT-FILTER-MITARBEITER" hinzu und ordnen Sie es unter Aktionen dem Content-Filter-Profil MITARBEITER zu:



10 Bestimmen Sie für das Aktions-Objekt CONTENT-FILTER-MITARBEITER eine Regel:



11 Ordnen Sie der Regel CF- MITARBEITER unter **Aktionen** das Aktionsobjekt CONTENT- FILTER- MITARBEITER zu:

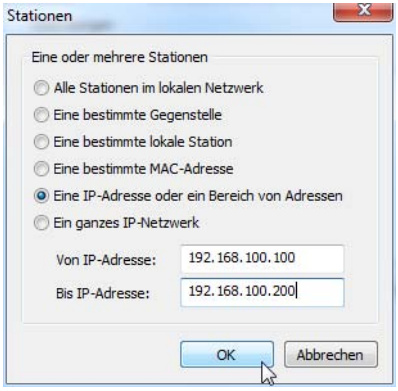


12 Bestimmen Sie nun weitere Details der Regel, z.B. kann eine Regel nur für einen bestimmten IP- Bereich gelten. Klicken Sie für diese Einstellung auf

DE

Stationen und bestimmen Sie z.B. einen Bereich von IP-Adressen für den diese Regel gelten soll.

Mit diesen Details der Firewall-Regel bestimmen Sie die Kriterien, nach denen die Nutzer einem bestimmten Content-Filter-Profil zugeordnet werden. Verwenden Sie hier also die Kriterien, mit denen Sie die unterschiedlichen Nutzergruppen unterscheiden können.



Damit sind die Einstellungen für Ihr Content-Filter-Profil MITARBEITER abgeschlossen. Die Konfiguration für Ihr Content-Filter-Profil AZUBIS können Sie in der gleichen Weise vornehmen.