LCOS 10.92

LANCOM Security Essentials

05/2025

LANCOM SYSTEMS

Inhalt

Copyright

© 2025 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity, LANCOM Service LANcare, LANCOM Active Radio Control und AirLancer sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS) finden Sie auf der WEBconfig des Geräts unter dem Menüpunkt „Extras > Lizenzinformationen“. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage über einen Download-Server bereitgestellt.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (*www.openssl.org*).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Einleitung

Mit den LANCOM Security Essentials 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.

Die LANCOM Security Essentials sind ein intelligenter Webseitenfilter und arbeiten dynamisch. Sie kontaktieren einen Bewertungsserver, der gemäß den von Ihnen ausgewählten Kategorien die Bewertung der Internetseiten zuverlässig und korrekt vornimmt.

Die Funktion der LANCOM Security Essentials 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 die LANCOM Security Essentials nicht umgehen, indem sie die IP-Adresse zu einer Webseite ermitteln und diese in den Browser eingeben. Die LANCOM Security Essentials prüfen sowohl unverschlüsselte (HTTP) als auch verschlüsselte Webseiten (HTTPS).

Das BPjM-Modul ein Bestandteil der LANCOM Security Essentials oder separat über die Software-Option LANCOM BPjM Filter Option erhältlich.. Das BPjM-Modul wird von der Bundeszentrale für Kinder- und Jugendmedienschutz herausgegeben und sperrt Domains, die Kindern und Jugendlichen in Deutschland nicht zugänglich gemacht werden dürfen.

Die von Ihnen erworbene Lizenz für die LANCOM Security Essentials gilt für eine bestimmte Gerätekategorie und einen bestimmten Zeitraum (jeweils für ein Jahr oder drei Jahre). Die Anzahl der Nutzer ist unlimitiert. Sie werden rechtzeitig über den Ablauf Ihrer Lizenz informiert.

Sie können die LANCOM Security Essentials 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 klicken Sie auf den Link unterhalb von **Sie benötigen eine 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 vordefinierten Haupt- und Unterkategorien in Ihren LANCOM Security Essentials: 73 Kategorien sind zu 12 Gruppen thematisch zusammengefasst, z. B. „Pornographie“, „Shopping“ oder „Illegales“. Für jede dieser Gruppen lassen sich die enthaltenen Kategorien aktivieren oder deaktivieren. Die Unterkategorien für „Pornografie“ sind z. B. „Pornografie“, „Sex-Spielzeuge“, „Sexuelle Inhalte“, „Nacktheit“, „Dessous“ und „Sexuelle Aufklärung“.

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 der LANCOM Security Essentials werden sinnvolle Standardeinstellungen automatisch eingerichtet, die für den ersten Start nur aktiviert werden müssen. In weiteren Schritten können Sie das Verhalten der LANCOM Security Essentials weiter an Ihren speziellen Anwendungsfall anpassen.

Auch für das BPjM-Modul werden sinnvolle Standardeinstellungen automatisch eingerichtet. So existiert in der IPv4- bzw. IPv6-Firewall eine Default-Firewall-Regel mit dem System-Objekt „BPJM“ als Zielstation. Definieren Sie als Quell-Stationen die Netzwerke, die durch das BPjM-Modul geschützt werden sollen. Durch Aktivierung der Regel wird das BPjM-Modul gestartet.

2 Voraussetzungen für die Benutzung der LANCOM Security Essentials

Folgende Voraussetzungen müssen erfüllt sein, damit Sie die LANCOM Security Essentials benutzen können:

1. Die LANCOM Security Essentials Option ist aktiviert.
2. Die Firewall muss aktiviert sein.
3. Eine Firewall-Regel muss das Content-Filter-Profil auswählen.
4. Das gewählte Content-Filter-Profil muss für jeden Zeitraum des 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 ungeprüfter Zugriff auf die Webseiten möglich.

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

3 Schnellstart

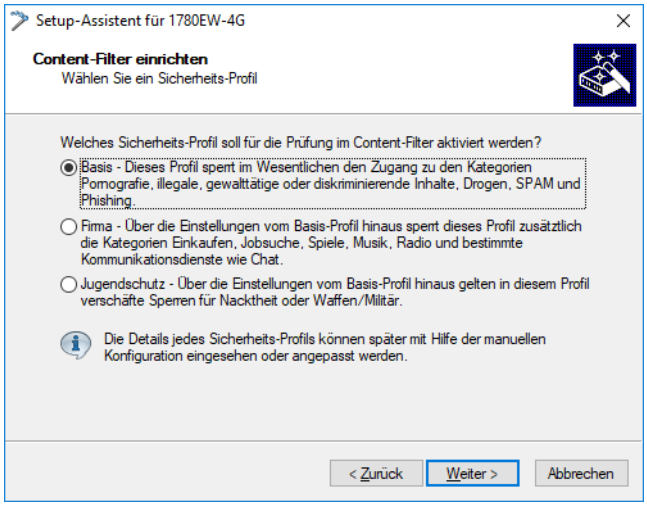
Nach der Installation der LANCOM Security Essentials sind alle Einstellungen für eine schnelle Inbetriebnahme vorbereitet.

Der Betrieb dder LANCOM Security Essentials kann durch die Datenschutzrichtlinien in Ihrem Land oder Betriebsvereinbarungen in Ihrem Unternehmen eingeschränkt sein. Bitte prüfen Sie vor Inbetriebnahme die geltenden Regelungen.

In LANconfig finden Sie die Einstellungen der LANCOM Security Essentials unter der Bezeichnung **Content Filter**.

Aktivieren Sie den 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 verschärfte Sperren für Nacktheit oder Waffen.

   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. Der Assistent aktiviert den Content Filter für den Zeitrahmen ALWAYS.

4 Die Standardeinstellungen im Content Filter

In der Standardeinstellung sind im Content Filter folgende Elemente angelegt:

Firewall-Regel

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

Firewall-Aktions-Objekte

Es existieren drei Firewall-Aktions-Objekte:

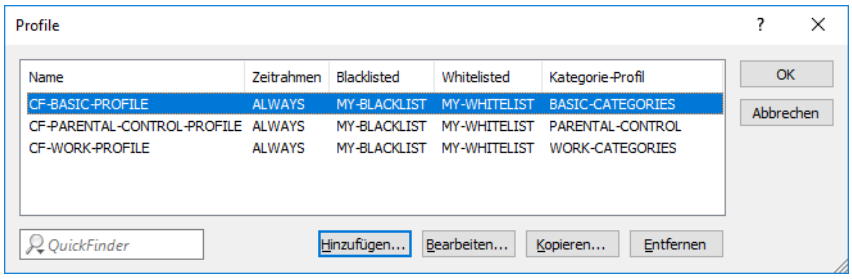
- CONTENT-FILTER-BASIC
- CONTENT-FILTER-WORK
- CONTENT-FILTER-PARENTAL-CONTROL

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 (z. B. 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.



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

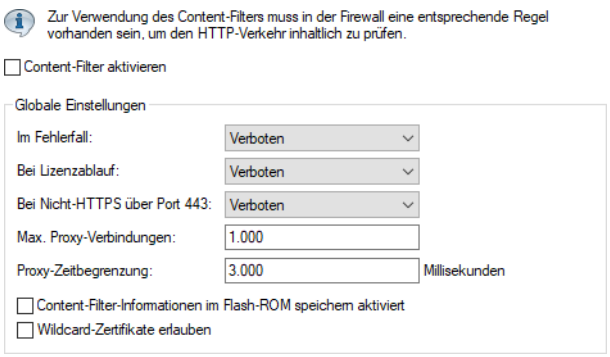
Die voreingestellte Whitelist hat den Namen MY-WHITELIST und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung erlaubt werden sollen.

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.

5 Allgemeine Einstellungen

Die globalen Einstellungen des Content Filters nehmen Sie in LANconfig unter **Content-Filter** > **Allgemein** vor:



Content Filter aktivieren

Hier können Sie den 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.

Bei Lizenzablauf

Die Lizenz zur Nutzung der LANCOM Security Essentials gilt für einen bestimmten Zeitraum. Sie werden jeweils 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz an die auslaufende Lizenz erinnert (an die E-Mailadresse, die in LANconfig konfiguriert ist unter **Meldungen** > **Allgemein** > **E-Mail-Adressen** > **Für Lizenz-Ablauf-Erinnerung**.

Hier können Sie bestimmen, ob Webseiten nach Ablauf der Lizenz blockiert oder ungeprüft durchgelassen werden sollen. 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.

Damit die Erinnerung auch tatsächlich an die angegebene E-Mailadresse versendet wird, müssen Sie das entsprechende SMTP-Konto konfigurieren.

Nicht-HTTPS-Traffic über Port 443

Verboten

Lässt Nicht-HTTPS-Traffic über Port 443 nicht zu.

Erlaubt

Lässt Nicht-HTTPS-Traffic über Port 443 zu.

Der TCP-Port 443 ist standardmäßig ausschließlich für HTTPS-Verbindungen reserviert.

Einige Applikationen, die nicht HTTPS nutzen, verwenden dennoch TCP-Port 443. Für diesen Fall haben Sie hier die Möglichkeit, den TCP-Port 443 auch für Nicht-HTTPS-Verbindungen zu öffnen.

Falls Sie Nicht-HTTPS-Verbindungen über Port 443 zulassen, wird der Traffic nicht weiter klassifiziert, sondern ganz pauschal zugelassen. Per Default werden Nicht-HTTPS-Verbindungen über Port 443 nicht zugelassen.

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. Es wird eine Benachrichtigung ausgelöst, wenn diese Anzahl überschritten wird. Die Art der Benachrichtigung können Sie unter **Content Filter** > **Optionen** > **Ereignisse** einstellen.

Proxy-Zeitbegrenzung

Stellen Sie hier die Zeit in Millisekunden ein, die der Proxy maximal für die Bearbeitung benötigen darf. Wird diese Zeit überschritten, wird dies durch eine entsprechende Zeitüberschreitungs-Fehlerseite quittiert.

Content-Filter-Informationen im Flash-ROM speichern aktiviert

Wenn Sie diese Option aktivieren, können Sie die Content-Filter-Informationen zusätzlich im Flash-ROM des Gerätes speichern.

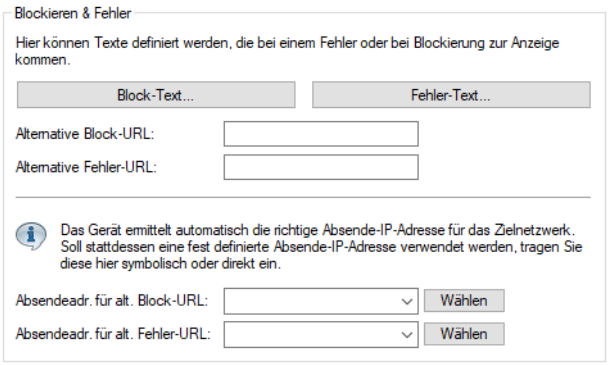
Wildcard-Zertifikate erlauben

Bei Webseiten mit Wildcard-Zertifikaten (bestehend aus CN-Einträgen wie z. B. `*.mydomain.de`) wird durch das Einschalten dieser Funktion die Haupt-Domain (`mydomain.de`) zur Prüfung herangezogen. Die Prüfung erfolgt dabei in dieser Reihenfolge:

- Prüfung des Servernamens im „Client Hello“ (abhängig vom verwendeten Webbrowser)
- Prüfung des CN im empfangenen SSL-Zertifikat
- Einträge mit Wildcards werden dabei ignoriert
- Ist der CN nicht verwertbar, wird das Feld „Alternative Name“ ausgewertet
- DNS Reverse Lookup der zugehörigen IP-Adresse und Prüfung des so erlangten Hostnamens
- Sind im Zertifikat Wildcards enthalten, wird stattdessen die Haupt-Domain geprüft (entspricht der oben beschriebenen Funktion)
- Prüfung der IP-Adresse

6 Einstellungen für das Blockieren

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



LANconfig: **Content-Filter** > **Blockieren / Override** > **Blockieren 6amp; Fehler**

Kommandozeile: **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 Block-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

Alternative Fehler-URL:

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle eines Fehlers 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 Fehler-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

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

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.

Absendeadr. für alt. Fehler-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

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

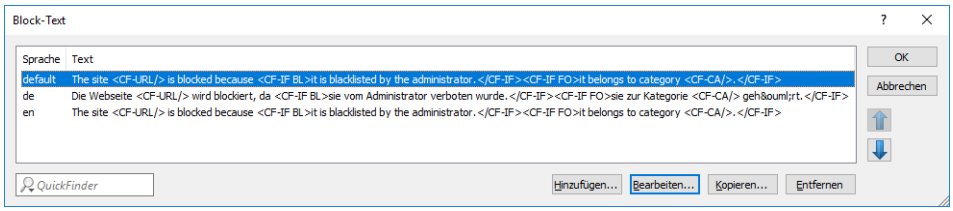
Default:

- leer

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

6.1 Block-Text

Hier können Sie einen Text definieren, der bei Blockierung angezeigt wird. Für unterschiedliche Sprachen kann jeweils ein eigener Block-Text definiert wird. Die Auswahl des verwendeten Block-Textes wird anhand der 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 eingestellte 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 vordefinierte 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 Block-Text für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Block-Text 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
- <CF-IF att1 att2> … </CF-IF> zum Ein- und Ausblenden von Teilen des HTML-Dokuments. Die 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.

- OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

  Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Attribut nur sinnvoll, wenn Sie eine alternative Block-URL konfiguriert haben.

Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mindestens 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 Block-Text nur maximal 254 Zeichen lang sein darf.

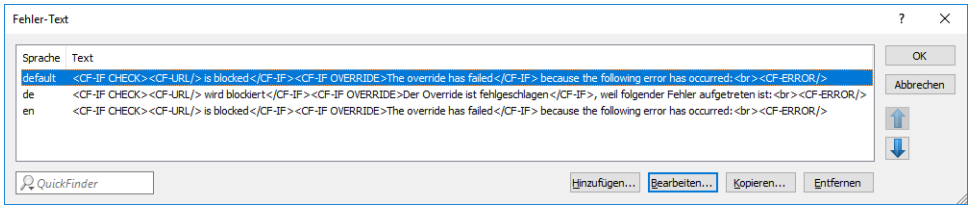
- Beispiel:

  <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.

6.2 Fehler-Text

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



Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellte 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 vordefinierte 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 Fehler-Text für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Fehler-Text 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:

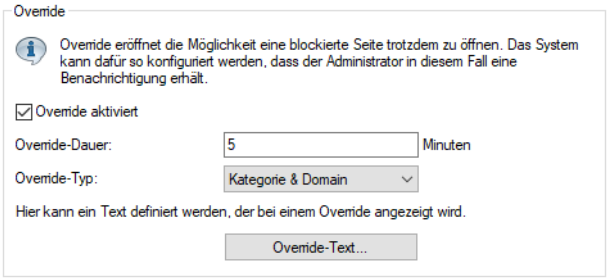
  <CF-URL/> wird verboten, weil ein Fehler aufgetreten ist:
<CF-ERROR/>

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

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. Wenn der Override-Typ „Domain" aktiviert ist, wird die Domain freigeschaltet.

Die Einstellungen für die Override-Funktion finden Sie hier:



LANconfig: **Content-Filter** > **Blockieren / Override** > **Override**

Kommandozeile: **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 wieder 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

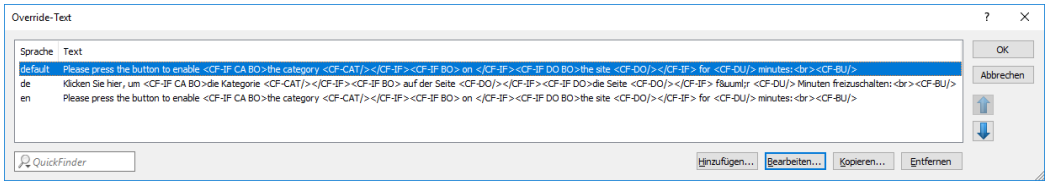
Während der Override-Dauer sind alle URLs unter der besuchten Domain erlaubt, egal zu welchen Kategorien sie gehören.

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.

7.1 Override-Text

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



Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellte 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 vordefinierte 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 Override-Text für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Block-Text 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.
- <CF-IF att1 att2> … </CF-IF> zum Ein- und Ausblenden von Teilen des HTML-Dokuments. Die Attribute sind:
  - 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>

8 Profile des Content Filters

Unter **Content-Filter** > **Profile** 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.

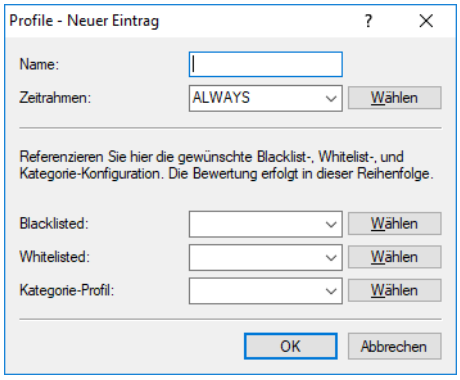
Um verschiedene Zeiträume unterschiedlich zu definieren, werden mehrere Content-Filter-Profileinträge mit dem gleichen Namen angelegt. Das Content-Filter-Profil besteht dann aus der Summe aller Einträge mit dem gleichen Namen.

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

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

8.1 Profile

Die Einstellungen für die Profile finden Sie hier:



LANconfig: **Content-Filer** > **Profile** > **Profile**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Profile** > **Profile**

Name

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

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**

Kommandozeile: **Setup** > **Zeit** > **Zeitrahmen**

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

Mögliche Werte:

- Always
- Never
- Name eines Zeitrahmenprofils

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

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

Kategorie-Profil

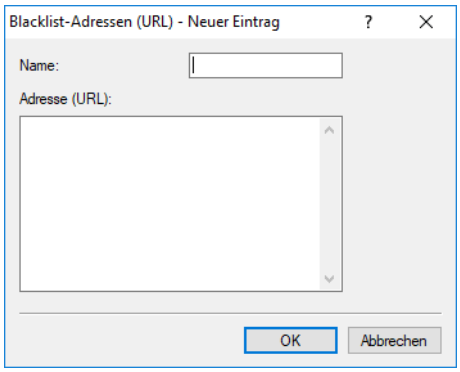
Name des Kategorie-Profils, das für dieses Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Kategorietabelle ausgewählt werden.

Mögliche Werte:

- Name eines Kategorie-Profils
- Neuer Name

8.2 Blacklist-Adressen (URL)

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



LANconfig: **Content-Filer** > **Profile** > **Blacklist-Adressen (URL)**

Kommandozeile: **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

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:

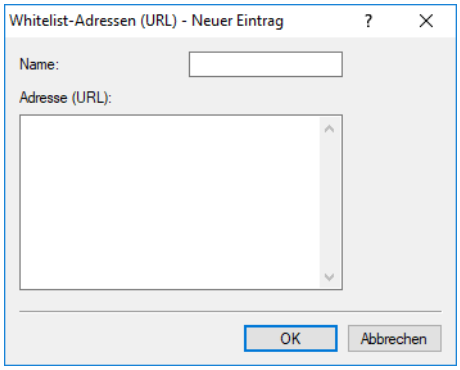
- * für mehrere beliebige Zeichen (z. B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.com, www.lancom.eu, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)

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.

8.3 Whitelist-Adressen (URL)

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



LANconfig: **Content-Filer** > **Profile** > **Whitelist-Adressen (URL)**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Profile** > **Whitelists**

Name

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

Mögliche Werte:

- Name einer Whitelist

Adresse (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:

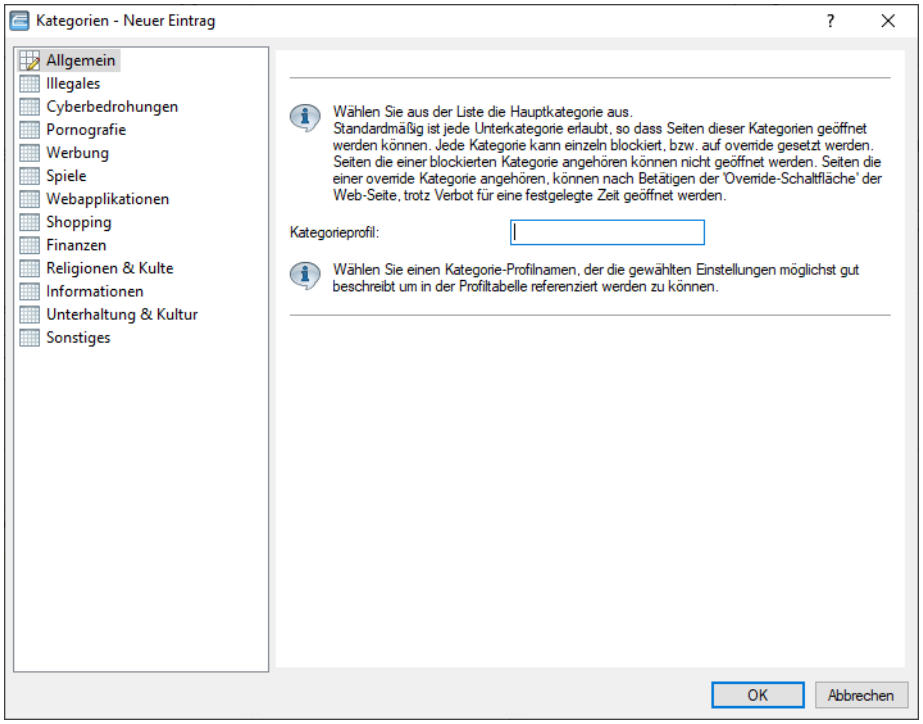
- * für mehrere beliebige Zeichen (z. B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.com, www.lancom.eu, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)

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.

8.4 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-Filer** > **Profile** > **Kategorien**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Profile** > **Kategorieprofile**

Kategorieprofil

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

Mögliche Werte:

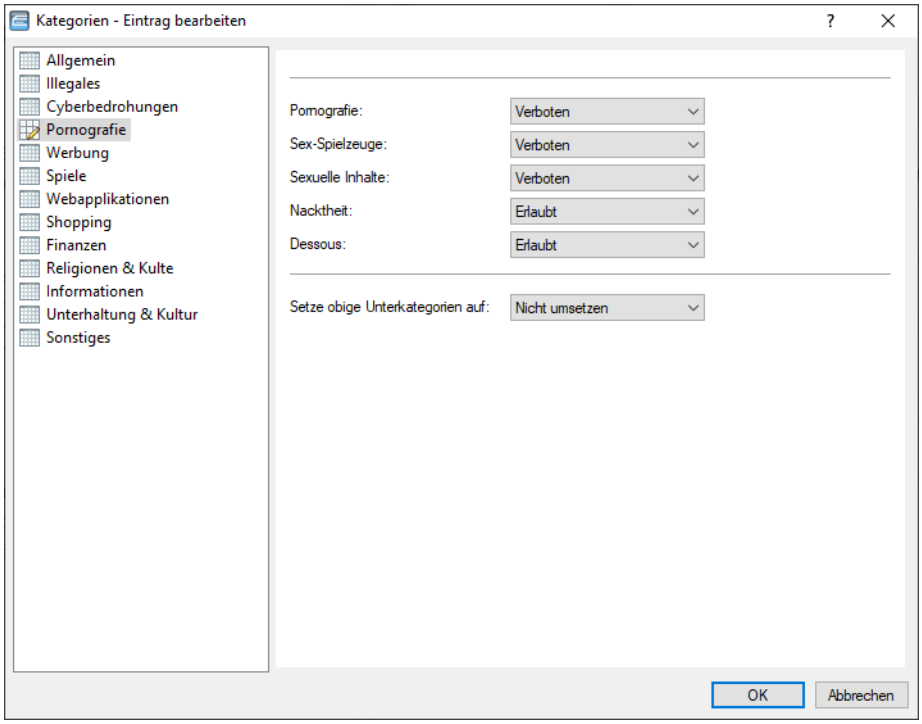
- Name eines Kategorieprofils

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:

- Illegales
- Cyberbedrohungen
- Pornografie
- Werbung
- Spiele
- Webapplikationen
- Shopping
- Finanzen
- Religionen & Kulte
- Informationen
- Unterhaltung & Kultur
- Sonstiges



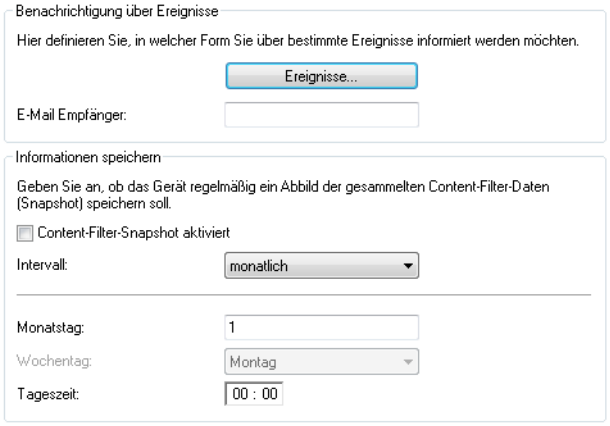
Das Kategorieprofil muss anschließend zusammen mit einem Zeitrahmen einem Content-Filter-Profil zugewiesen werden, um aktiv zu werden.

Mögliche Werte:

- Erlaubt, Verboten, Override

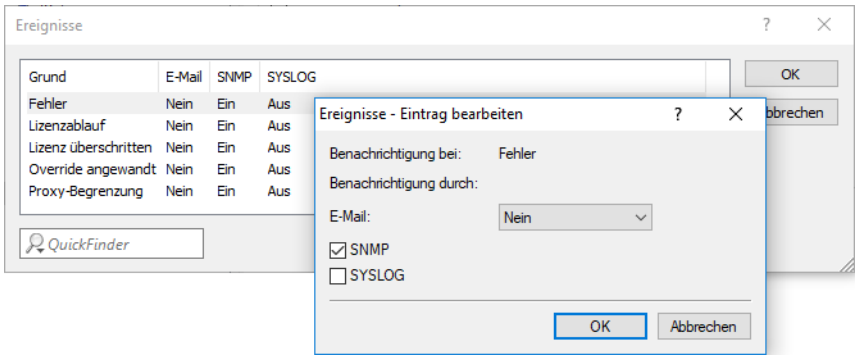
9 Optionen des Content Filters

Unter **Content-Filter** > **Optionen** können Sie einstellen, ob Sie über Ereignisse benachrichtigt werden und wo die Informationen des Content Filters gespeichert werden sollen.



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, ob und in welcher Menge Meldungen ausgegeben werden sollen.



E-Mail

Definieren Sie hier, ob und wie eine E-Mail-Benachrichtigung erfolgt:

- **Nein**

  Für dieses Ereignis erfolgt keine E-Mail-Benachrichtigung.

- **Unverzüglich**

  Die Benachrichtigung erfolgt, sobald das Ereignis eintritt.

- **Täglich**

  Die Benachrichtigung erfolgt einmal am Tag.

Die folgenden Ereignisse stehen für Benachrichtigungen zur Verfügung:

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

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 Schnappschuss monatlich, wöchentlich oder täglich angefertigt werden soll.

Mögliche Werte:

- Monatlich
- Wöchentlich
- Täglich

Monatstag

Ist eine monatliche Ausführung des Schnappschuss gewünscht, wählen Sie hier den Tag, an dem der Schnappschuss angefertigt werden soll. Mögliche Werte:

- 1-31

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

Wochentag

Ist eine wöchentliche Ausführung des Schnappschuss gewünscht, selektieren Sie hier den Wochentag, an dem der Schnappschuss angefertigt werden soll. Mögliche Werte:

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

Tageszeit

Ist eine tägliche Ausführung des Schnappschuss gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein. Mögliche Werte:

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

10 Zusätzliche Einstellungen für den Content Filter

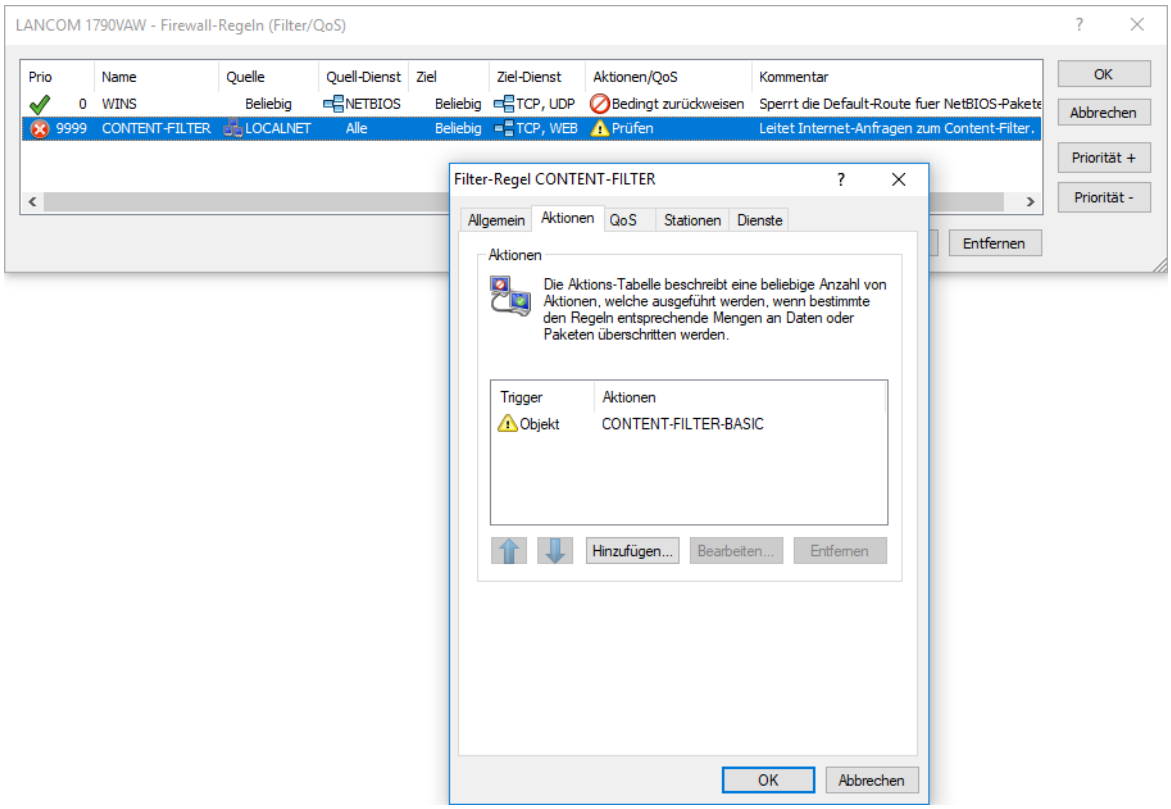
10.1 Firewall-Einstellungen für den Content Filter

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

LANconfig: **Firewall/QoS** > **Allgemein**

Kommandozeile: **Setup** > **IP-Router** > **Firewall**

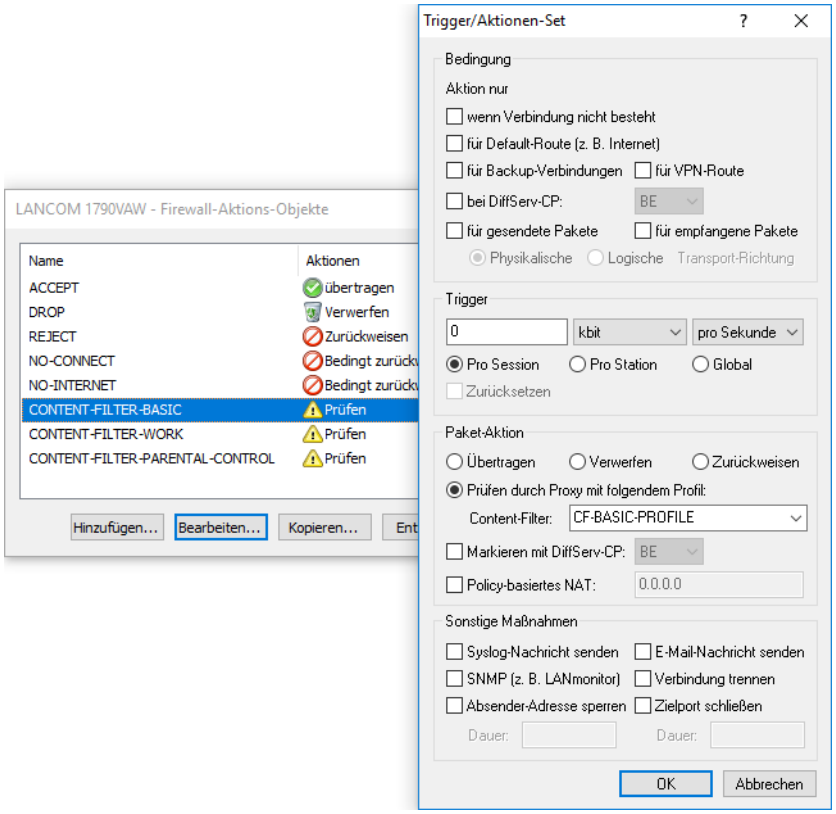
In der Default-Einstellung finden Sie die Firewall-Regel CONTENT-FILTER, die auf das Aktionsobjekt CONTENT-FILTER-BASIC zurückgreift:



Die Firewall-Regel sollte auf die Zieldienste HTTP und HTTPS beschränkt werden, damit nur ausgehende HTTP- und HTTPS-Verbindungen erfasst werden. Ohne diese Einschränkung werden alle Pakete über den Content Filter geprüft, was zu einer Beeinträchtigung der Performance 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:



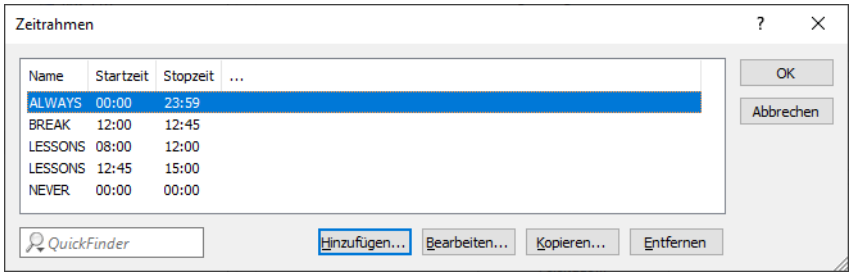
Beispiel: Beim Öffnen einer Webseite durchlaufen die Datenpakete die Firewall und werden von der Regel CONTENT-FILTER erfasst. Das Aktionsobjekt CONTENT-FILTER-BASIC prüft die Datenpakete mit dem Content-Filter-Profil CONTENT-FILTER-BASIC.

10.2 Zeitrahmen

Zeitrahmen werden beim Content Filter 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.

Zeitrahmen können auch verwendet werden, um eine WLAN-SSID nicht dauerhaft auszustrahlen. Dazu kann dieser bei den logischen WLAN-Einstellungen hinzugefügt werden.

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



LANconfig: **Datum/Zeit** > **Allgemein** > **Zeitrahmen**

Kommandozeile: **Setup** > **Zeit** > **Zeitrahmen**

Name

Hier muss der Name des Zeitrahmens angegeben werden, über den dieser im Content-Filter-Profil oder bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil.

Mögliche Werte:

- Name eines Zeitrahmens

Startzeit

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

Mögliche Werte:

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

Stoppzeit

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

Mögliche Werte:

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

Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

Wochentage

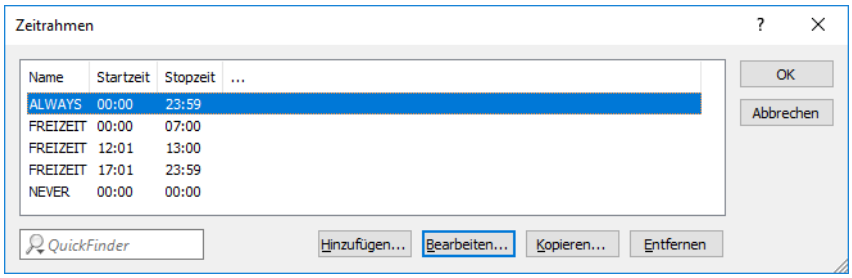
Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

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

Die Feiertage werden unter **Datum/Zeit** > **Allgemein** > **Feiertage** eingestellt.

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



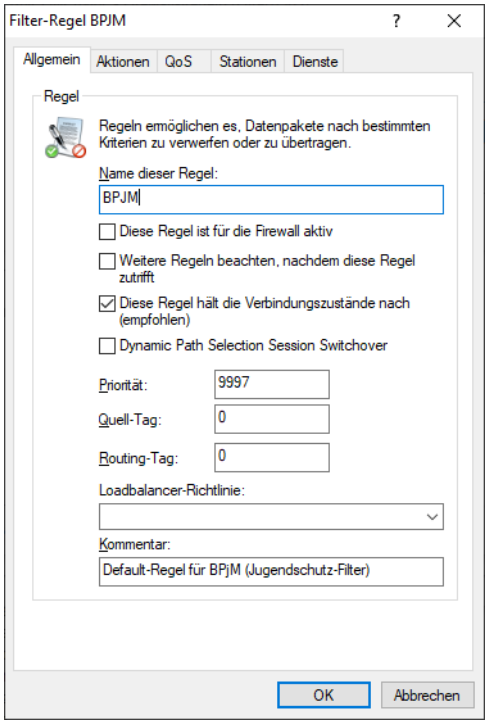
11 BPjM-Modul

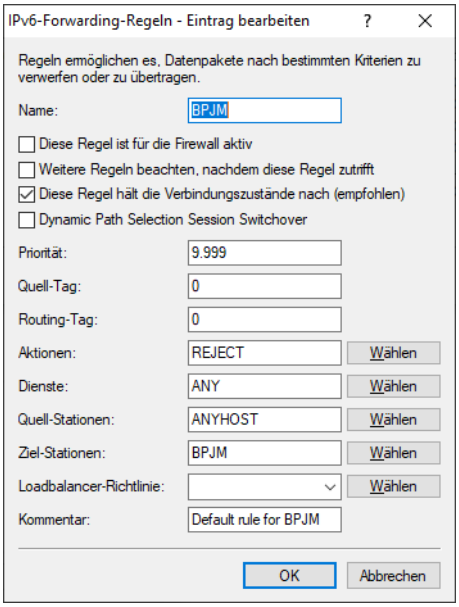
Das BPjM-Modul wird von der Bundeszentrale für Kinder- und Jugendmedienschutz herausgegeben und sperrt Webseiten, die Kindern und Jugendlichen in Deutschland nicht zugänglich gemacht werden dürfen. Diese Funktion ist besonders für Schulen und Bildungseinrichtungen mit minderjährigen Schülern relevant. Damit sind DNS-Domains, deren Inhalte offiziell als jugendgefährdend eingestuft werden, für die entsprechende Zielgruppe in Deutschland nicht erreichbar. Eine automatische und regelmäßige Aktualisierung und Erweiterung dieser Auflistung ist dabei gewährleistet. Das BPJM-Modul sperrt DNS-Domains die auf der offiziellen Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) stehen. Eine Sperrung nach Kategorie oder Override (Erlauben) ist hierbei nicht möglich.

Das BPJM-Modul ist Teil der LANCOM Security Essentials Option oder separat über die Software-Option LANCOM BPjM Filter Option erhältlich.

In der IPv4- bzw. IPv6-Firewall existiert dazu eine Default-Firewall-Regel, die aktiviert werden kann und pro Netz konfiguriert werden kann. So ist beispielsweise möglich, nur das Schülernetz mit diesem Filter auszustatten, andere Netze aber davon auszunehmen.

In der IPv6-Firewall existiert eine neue Default-Regel BPJM, die standardmäßig deaktiviert ist mit dem System-Objekt „BPJM“ als Zielstation. In der IPv4-Firewall existiert dazu analog eine Regel. Definieren Sie als Quell-Stationen die Netzwerke, die durch das BPjM-Modul geschützt werden sollen.





Weitere Einstellungen finden Sie in LANconfig unter **Sonstige Dienste** > **Dienste** > **BPjM-Filter**.

Absende-Adresse

Absende-Adresse, die vom BPjM-Modul verwendet wird, um den Server für BPjM-Signatur-Updates zu erreichen.

11.1 Einsatzempfehlungen

Sollen Content-Filter und BPJM-Filter gemeinsam verwendet werden, müssen beide Regeln mit unterschiedlichen Prioritäten konfiguriert werden, so dass diese nacheinander durchlaufen werden.

Ebenso muss bei der ersten Regel darauf geachtet werden, dass der Punkt „Weitere Regeln beachten, nachdem diese Regel zutrifft“ aktiviert ist.

In seltenen Fällen kann es dazu kommen, dass das BPJM-Modul gewünschte Domains blockiert, da nur (DNS-)Domains und keine URL-Verzeichnisebenen aufgrund von TLS geprüft werden können. In diesem Fall können diese gewünschten Domains in der „BPJM-Allow-Liste“ hinzugefügt werden, z. B. *.example.com.

Der LANCOM Router muss als DNS-Server bzw. DNS-Forwarder im Netz dienen, d. h. Clients im lokalen Netzwerk müssen den Router als DNS-Server verwenden. Zusätzlich muss die direkte Nutzung von DNS-over-TLS und DNS-over-HTTPS (ggf. browserintern) mit externen DNS-Servern durch Clients verhindert werden.

Dies kann wie folgt erreicht werden:

- Der DHCP-Server muss die IP-Adresse des Routers als DNS-Server verteilen (wird standardmäßig vom Internet-Wizard eingerichtet)
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern verhindern, z. B. durch Sperrung des ausgehenden Ports 53 (UDP) für Clients aus dem entsprechenden Quellnetzwerk
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern mit Unterstützung von DNS-over-TLS verhindern, z. B. durch Sperrung des ausgehenden Ports 853 (TCP) für Clients aus dem entsprechenden Quellnetzwerk
- DNS-over-HTTPS (DoH) im Browser deaktivieren

Hinweise zur Synchronisierung der DNS-Datenbank der Firewall:

Da die Firewall ihre Informationen aus den DNS-Anfragen der Clients lernt, kann es in bestimmten Situationen dazu kommen, dass die DNS-Datenbank noch nicht vollständig ist. Dies kann in folgenden Situationen passieren:

- Es wird eine neue Firewall-Regel hinzugefügt, der Client hat aber noch einen DNS-Eintrag zwischengespeichert
- Kurz nach Neustart des Routers und der Client hat aber noch einen DNS-Eintrag zwischengespeichert

In diesen Fällen hilft ein Leeren des DNS-Cache auf dem Client, ein Reboot des Clients oder ein Timeout des DNS-Eintrags auf dem Client.

Wenn unterschiedliche DNS-Namen auf dieselbe IP-Adresse aufgelöst werden, dann können diese nicht unterschieden werden. In diesem Fall trifft immer die erste Regel zu, die einen dieser DNS-Namen referenziert. Das sollte bei großen Dienstanbietern kein Problem sein. Bei kleinen Webseiten, die vom selben Anbieter gehostet werden, könnte es jedoch auftreten.