



## LANCOM Content Filter Option

### Optimaler Schutz vor Missbrauchs des Netzwerks

Der LANCOM Content Filter bietet eine effiziente Lösung, um Netzwerke vor Missbrauch zu bewahren und so die unangemessene Nutzung von Bandbreite sowie das Herunterladen von Malware zu vermeiden. Durch die Blockierung unerwünschter und illegaler Internet-Inhalte wird gleichzeitig die Geschäftsintegrität geschützt und das Haftungsrisiko minimiert.

- › Kategoriebasierter Webfilter
- › Zeit- und profilbasierte Konfiguration
- › Umfangreiche Nutzungsstatistiken
- › Kategoriebasierte Overrides für Webseiten einstellbar
- › Additive Lizenzen für 10, 25 oder 100 Benutzer
- › Erhältlich für LANCOM VPN-Router, Central Site VPN Gateways und WLAN-Controller
- › Einfach das vorhandene Gerät aufrüsten und Hardware-Komponenten einsparen

# LANCOM Content Filter Option

## Schutz vor Missbrauch des Netzwerks

Die Bandbreite des Netzwerks bleibt mit dem LANCOM Content Filter in vollem Umfang dem Geschäftsbetrieb vorbehalten und Webseiten mit Spyware, Phishing, Viren etc. werden sicher blockiert. Hierfür nutzt der Content Filter eine datenbankgestützte Webfilter-Technologie, bei der ein externer Bewertungsserver die angeforderten Websites online auf ihre tatsächlichen Inhalte prüft. Der Administrator kann frei konfigurieren, welche thematischen Kategorien gesperrt werden und welche zugänglich sind. Drei vorgefertigte Sicherheitsprofile – Basis, Firma, Jugendschutz – bieten darüber hinaus eine schnelle und effiziente Einführung dieser Lösung.

## Individuelle zeit- und profilbasierte Konfiguration

In einem Netzwerk können anhand des LANCOM Content Filters Zugriffsrechte auf Internetseiten zeitlich und personenbezogen frei konfiguriert werden. So können z.B. während der Mittagspausenzeit Inhalte frei geschaltet werden, die während der Kernarbeitszeit gesperrt sind. Ebenso ist es möglich, für Nutzer individuelle Profile anzulegen, sodass Internetinhalte, die beispielsweise für den Arbeitsplatz relevant sind, für die betreffenden Personen freigeschaltet werden.

## Alles im Blick dank umfangreicher Statistiken

Der LANCOM Content Filter bietet umfangreiche Statistiken an. So können über einen einstellbaren Zeitraum z.B. Top-10 Listen erstellt werden, die den Zugriff auf erlaubte Websites sowie den Versuch auf blockierte und Override-URLs aufzeigen. Auch die Auswertung nach Kategorien ist möglich. Alle Statistiken werden dabei nicht personenbezogen erstellt, sodass die Einhaltung strenger Datenschutzrichtlinien gewährleistet bleibt.

## Kategoriebasierte Overrides für Webseiten

Der Override-Button ermöglicht blockierte Webseiten temporär aufzurufen. Damit sind kurzzeitige Zugriffe auf eigentlich gesperrte URLs möglich, ohne die Konfiguration erneut anpassen zu müssen. Der Override kann pro Kategorie aktiviert und via E-Mail, SYSLOG und SNMP überwacht werden. Die Nutzung bietet sich vor allem dann an, wenn die User aus begründeten Anlässen bestimmte Websites aufrufen möchten oder müssen.

## Effektiver Schutz für jede Größenordnung

Die Lizenzierung des Content Filters erfolgt benutzerbasierend. Es werden durch das LANCOM Gerät nur die IP-Adressen gezählt, die auf geblockten Content durch den Filter zugreifen wollen. Die Lizenzierung in verschiedenen Größenordnungen ermöglicht so eine genaue Anpassung an das Netzwerk sowie – bei Bedarf – eine komfortable Erweiterung.

## Einfach aufrüsten

Die LANCOM Software-Optionen machen aus einem einfachen Netzwerk eine auf individuelle Bedürfnisse abgestimmte und kostengünstige Lösung. Einmal auf die vorhandene Hardware aufgespielt, erweitern sie das Netzwerk um die gewünschte Funktion. Der Vorteil: Es sind keine weiteren Hardware-Komponenten erforderlich. Das reduziert die Anschaffungskosten und den Administrationsaufwand des gesamten Netzwerks. Ein echter Mehrwert im Hinblick auf die Zukunftsfähigkeit, denn dank der Optionen wird das Netzwerk zu einer einzigartigen, skalierbaren Netzwerklösung.

# LANCOM Content Filter Option

Content Filter	
URL-Filter-Datenbank/Ratingsserver*	Weltweit redundante Ratingsserver der IBM Security Solutions zur Abfrage von URL-Klassifizierungen. Datenbank mit über 100 Millionen Einträgen, die etwa 10 Milliarden Webinhalte abdeckt. Täglich fast 150.000 Aktualisierungen durch Webcrawler, welche automatisiert Webseiten untersuchen und kategorisieren: durch Textklassifizierung mit optischer Zeichenerkennung, Schlüsselwortsuche, Bewertung von Häufigkeit und Wort-Kombinationen, durch Webseitenvergleich hinsichtlich Text, Bildern und Seitenelementen, durch Objekterkennung von speziellen Zeichen, Symbolen, Warenzeichen, verbotenen Bildern, durch Erkennung von Erotik und Nacktheit anhand der Konzentration von Hauttönen in Bildern, durch Struktur- und Linkanalyse, durch Malware-Erkennung in Binärdateien und Installationspaketen
URL-Prüfung*	Datenbankbasierte Online-Prüfung von Webseiten (HTTP/HTTPS). HTTPS-Webseiten werden durch die Entnahme von angesteuerten DNS-Namen aus HTTPS-Serverzertifikaten oder durch "Reverse DNS lookup" der IP-Adresse geprüft und ggfs. blockiert.
Kategorien/Kategorie-Profile*	Definition von Filterregeln pro Profil durch Zusammenstellen von Kategorie-Profilen aus 58 Kategorien, z.B. zur Einschränkung der Internetnutzung auf geschäftliche Anwendungen (Unterbinden privater Nutzung) oder Schutz vor jugendgefährdenden oder gefährlichen Inhalten wie z.B. Malware-Seiten. Übersichtliche Auswahl durch Zusammenstellung thematisch ähnlicher Kategorien zu Gruppen. Inhalte pro Kategorie erlauben, blockieren oder für Override freigeben
Override**	Für Kategorien kann ein Override vergeben werden, der es Anwendern fallweise erlaubt, eigentlich gesperrte Seiten durch manuelle Bestätigung zu laden. Der Override kann zeitlich beschränkt für die Kategorie, die Domäne oder eine Kombination aus beidem ausgesprochen werden. Möglichkeit zur Benachrichtigung eines Administrators im Fall von Overrides
Black-/Whitelist	Manuell konfigurierbare Listen zum expliziten Erlauben (Whitelist) oder Verbieten (Blacklist) von Webseiten pro Profil, unabhängig von der Bewertung durch den Ratingserver. Platzhalter (Wildcards) zur Definition von Gruppen von Seiten oder Filtern von Unterseiten
Profile	Zusammenfassen von Zeitrahmen, Black-/Whitelists und Kategorie-Profilen zu getrennt aktivierbaren Profilen für Content Filter Aktionen. Werksseitig aktiviertes Default-Profil mit Standard-Einstellungen zum Blocken von rassistischen, pornografischen, kriminellen, extremistischen Inhalten sowie anonymen Proxies, Waffen/Militär, Drogen, SPAM und Malware
Zeitrahmen	Flexible Definition von Zeitrahmen, um Profile zur Filterung in Abhängigkeit von Tageszeiten oder Wochentagen zu definieren, z. B. für Lockerung während Pausenzeiten für privates Surfen
Flexibel anwendbare Firewall-Aktion	Anwendung des Content Filters durch Content Filter Aktionen mit Auswahl des gewünschten Profils in der Firewall. Firewall-Regeln ermöglichen die flexible Anwendung eigener Profile für verschiedene Clients, Netze oder Verbindungen zu bestimmten Servern
Individuelle Rückmeldungen (bei blockiert, Fehler, Override)	Antwortseiten des Content Filters für blockierte Seiten, Fehler und Override können individuell gestaltet und durch Variablen mit aktuellen Informationen zu Kategorie, URL und Kategorisierung des Ratingservers versehen werden. Sprachabhängige Definition von Antwortseiten, je nach vom Anwender ausgewählter Anzeigesprache des Webbrowsers
Umleitung zu externen Webseiten	Alternativ zur Anzeige der geräteinternen Antwortseiten für blockierte Seiten, Fehler oder Override können auch Seiten von externen Webservern aufgerufen werden (Redirect)
Lizenzmanagement	Automatische Benachrichtigung vor Ablauf der Lizenz per E-Mail, LANmonitor, SYSLOG und SNMP-Trap. Aktivierung der nächsten Lizenz-Verlängerung zu beliebigem Zeitpunkt vor dem Ablauf der aktuellen Lizenz (Start des neuen Lizenzzeitraumes passend zum Ablauf der aktuellen Lizenz)
Statistiken	Anzeige der Anzahl der geprüften und gesperrten Webseiten je Kategorie in LANmonitor. Logging aller Content-Filter-Events in LANmonitor; tägliches, wöchentliches oder monatliches Anlegen einer Protokolldatei. Hitliste der meist aufgerufenen Seiten und Ratingergebnisse. Auswertung der Verbindungseigenschaften, minimalen, maximalen und durchschnittlichen Antwortzeiten des Ratingservers
Alarmierungen	Benachrichtigung bei Content-Filterung einstellbar via E-Mail, SNMP, SYSLOG sowie LANmonitor
Assistent für Standard-Konfigurationen	Assistent zur Einrichtung des Content Filters für typische Anwendungsszenarien in wenigen Schritten, inklusive Erzeugung der nötigen Firewall-Regeln mit entsprechender Aktion
*) Hinweis	Die Kategorisierung erfolgt durch IBM. Die jederzeitige Richtigkeit der Kategorisierungen können weder IBM noch LANCOM garantieren.
**) Hinweis	Die Override-Funktionalität steht nur für HTTP-Seiten zur Verfügung.
Nutzbar mit folgenden Geräten	
LANCOM 831A	Max. 25 Benutzer
LANCOM 1631E	Max. 25 Benutzer
LANCOM 178x	Max. 100 Benutzer
LANCOM IAP-(321)-3G	Max. 100 Benutzer
LANCOM IAP-4G	Max. 100 Benutzer
LANCOM OAP-3G	Max. 100 Benutzer

# LANCOM Content Filter Option

Nutzbar mit folgenden Geräten	
LANCOM 88x VoIP	Max. 100 Benutzer
LANCOM WLC 4006(+)	Max. 100 Benutzer
LANCOM WLC-4025+	Max. 400 Benutzer
LANCOM WLC-4100	Max. 400 Benutzer
LANCOM 7100(+) VPN	Max. 400 Benutzer
LANCOM 9100(+) VPN	Max. 400 Benutzer
LANCOM ISG-1000	Max. 1.000 Benutzer
LANCOM ISG-4000	Max. 1.000 Benutzer
LANCOM WLC-1000	Max. 1.000 Benutzer
Artikelnummer(n)	
LANCOM Content Filter +10 Benutzer, 1Jahr Laufzeit	61590
LANCOM Content Filter +25 Benutzer, 1Jahr Laufzeit	61591
LANCOM Content Filter +100 Benutzer, 1Jahr Laufzeit	61592
LANCOM Content Filter +10 Benutzer, 3Jahre Laufzeit	61593
LANCOM Content Filter +25 Benutzer, 3Jahre Laufzeit	61594
LANCOM Content Filter +100 Benutzer, 3Jahre Laufzeit	61595