Collax Web Security

Howto

Dieses Howto beschreibt die Einrichtung eines Web-Proxy-Servers als Web-Contentfilter.

Voraussetzungen

- Collax Business Server
- Collax Security Gateway
- Collax Platform Server inkl. Collax Modul Web Security

Optional

- Collax Surf Protection powered by Cobion
- Collax Virus Protection powered by Kasperky
- Collax AntiVir Protection powered by Avira

Ziel

Sollen in einem Netzwerk verschiedene Benutzergruppen unterschiedliche Berechtigungen für den Zugang und den Inhalt zum Internet erhalten, ist es erforderlich Web-Content-Filterregeln zu definieren. Diese Filterregeln können, je nach Anforderung, zu komplexen Regelwerken wachsen.

Dieses Dokument gibt Ihnen anhand eines praktischen Beispiels Hilfestellung für die prinzipielle Erstellung solcher Regelwerke auf einem Collax Business Server (CBS).

Aufgabe

Ein mittelständisches Unternehmen möchte für seine Mitarbeiter unterschiedliche Regeln für den Zugriff auf Webseiten geltend machen. Die Geschäftsleitung, sowie die Administratoren sollen vollen Zugriff auf alle Webseiten erhalten. Bei den Mitarbeitern sollen bestimmte Kategorien ausgeschlossen werden. Die Auszubildenden sollen nur auf wikipedia.org und auf die Firmenwebseite Zugriff haben. Des Weiteren soll der gesamte HTTP-Verkehr auf Viren untersucht werden. Hierzu kommt die Antivirenlösung Collax Virus Protection powered by Kaspersky zum Einsatz.

Lösung

Es gibt grundsätzlich 3 Möglichkeiten um das Regelwerk zu konfigurieren.

1. Authentifizierung direkt am Webproxy über Eingabe von Login und Passwort des Benutzers auf dem CBS.
2. Authentifizierung am Active Directory (AD) Server. Der Client meldet sich an der Windows Domäne an.

Der CBS muss Mitglied der Windowsdomäne sein. Auf dem AD Server müssen 3 Gruppen angelegt sein (für unser Beispiel), die alle Benutzer des Netzwerks enthält. d.h. es darf keinen Benutzer in der Windowsdomäne geben, der keiner dieser 3 Gruppen zugeordnet ist. Ansonsten hat dieser Benutzer die gleichen Berechtigungen wie die Administratoren-Gruppe.

3. Unterscheidung über die IP Adresse der einzelnen Clients. Hier ist keine Authentifizierung nötig.

In diesem Howto gehen wir nur auf die Lösung des Punktes 1 ein.

Status:Final Version:5.8 Datum: 27.10.2014

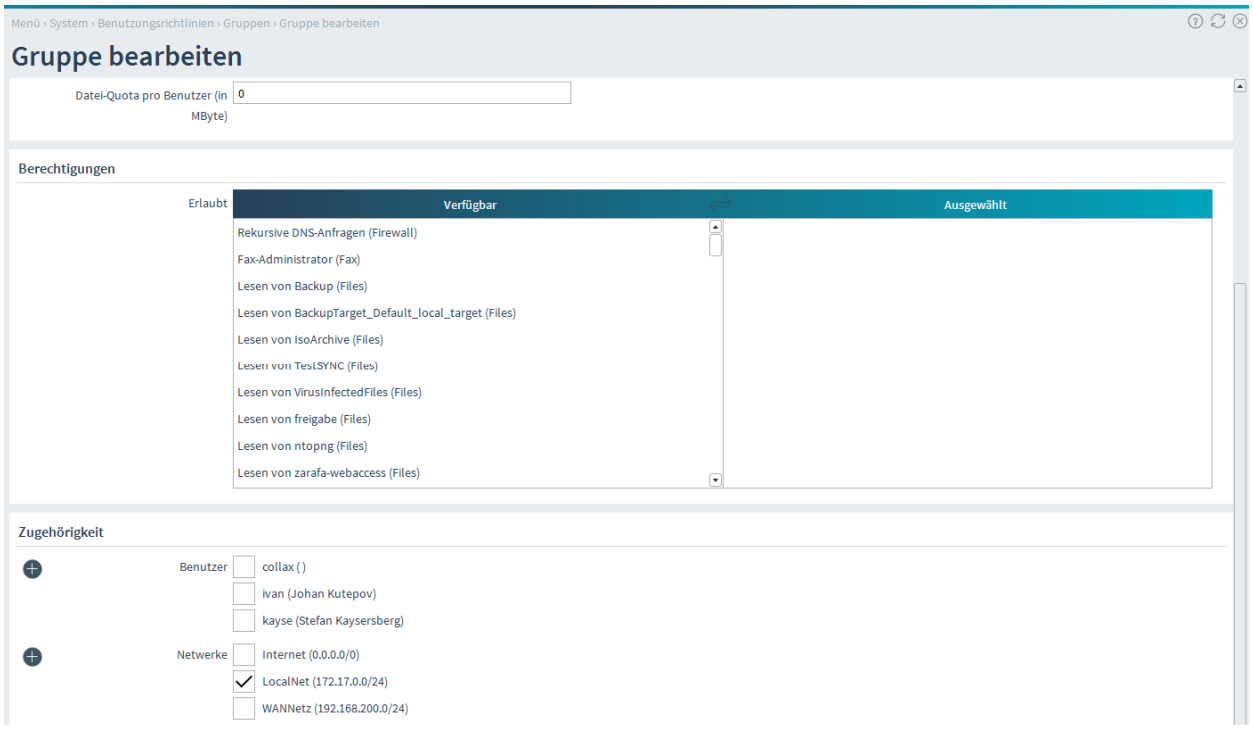
Zunächst werden 3 Gruppen angelegt:

- Proxy_GL
- Proxy_Mitarbeiter
- Proxy_Azubis

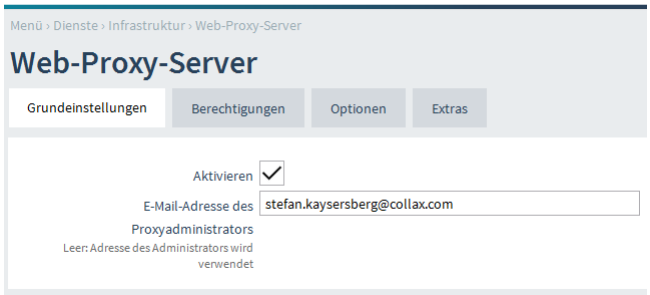
Angelegte Benutzer werden auf die Gruppen verteilt. Beachten Sie, dass Benutzer, die keiner Proxygruppe angehören die Berechtigungen einer dieser Gruppe erhalten. Welche das ist kann nicht genau bestimmt werden.

Wichtig Jeder Benutzer muss daher einer dieser Gruppen zugeordnet sein.

Mindestens einer Gruppe ist das lokale Netzwerk *Localnet* zuzuordnen.

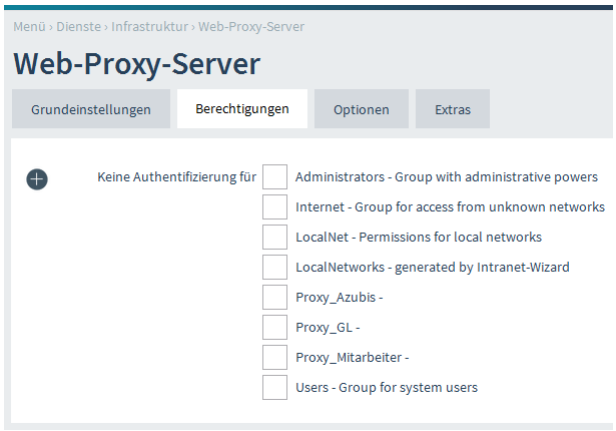


Anschließend wird der Web-Proxy unter *„Dienste → Infrastruktur → Webproxy → Web-Proxy-Server“* aktiviert und die Grundeinstellung vorgenommen.



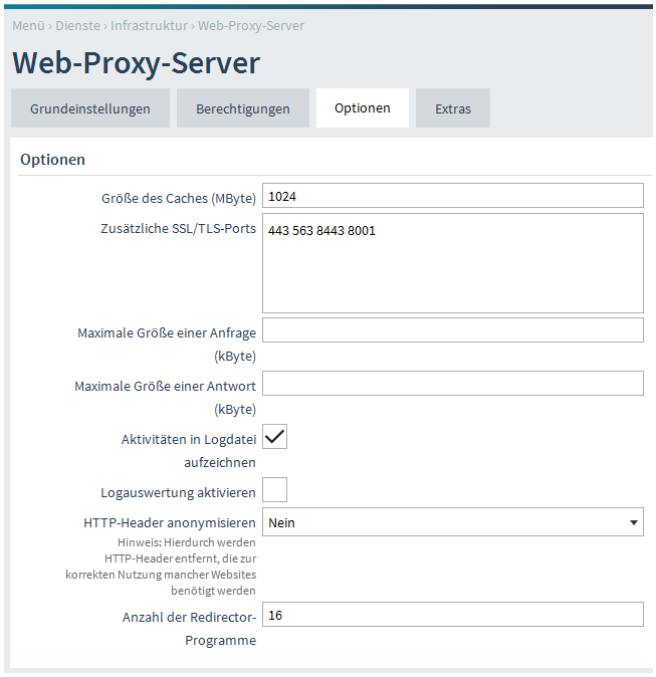
E-Mail-Adresse des Proxyadministrators Tritt ein Fehler auf, zeigt der Proxyserver eine Webseite mit einer Fehlermeldung an. Auf dieser Webseite wird die E-Mail-Adresse des lokalen Administrators angezeigt. Die Adresse wird in diesem Feld hinterlegt.

Beachten Sie, dass unter *Berechtigungen* keine Gruppen eingetragen werden dürfen, da wir den Web-Proxy mit Authentifizierung einrichten möchten



Grundeinstellungen

Im Bild unten sehen Sie die Grundkonfiguration des Web-Proxy-Servers.



Größe des Caches (MByte) Mit diesem Parameter wird die maximale Größe des Caches auf der Festplatte eingestellt. Dieser Wert sollte größer als 128 MByte sein. Der Maximalwert beträgt 10240 MB (10 GB). Je nach Geschwindigkeit des Plattensystems gibt es eine Grenze, bei deren Überschreitung der Cache langsamer wird. Übliche Werte liegen zwischen 512 MB und 2 GB.
Hinweis: Hier wird nur der reine Zahlenwert in Megabyte (ohne Einheit) angegeben.

Zusätzliche SSL/TLS-Ports Der HTTP-Proxy kann prinzipbedingt keine HTTPS-Anfragen cachen, da er die verschlüsselten Daten nicht lesen kann. Um dennoch HTTPS-Daten über den Proxy weiterleiten zu können, gibt es die Connect-Methode, mit der ein Client eine indirekte Verbindung zu einem HTTPS-Server aufnehmen kann.
Der HTTP-Proxy kann jedoch nicht prüfen, ob die Verbindung tatsächlich eine HTTPS-Verbindung ist. Darum sind für die Connect-Methode nur bestimmte Ports zugelassen, nämlich 443, 563 und 8443.

Hier können zusätzliche Ports angegeben werden, die für die Connect-Methode erlaubt sind. Zum Zugriff auf andere Collax-Server durch den Proxy muss hier etwa „8001“ zusätzlich eingetragen werden.

Maximale Größe einer Anfrage (kByte) Diese Einstellung gibt an, wie groß eine einzelne Anfrage an einen Webserver sein darf. Dies limitiert insbesondere die Größe von Dateien, die an einen Webserver geschickt werden können.
In der Voreinstellung ist dieses Feld leer, wodurch die Größe von Anfragen nicht beschränkt ist.

Maximale Größe einer Antwort (kByte) Diese Einstellung begrenzt die maximale Größe einer Datei, die über den Proxy heruntergeladen werden kann.
In der Voreinstellung ist dieses Feld leer, wodurch keine Größenbeschränkung existiert.
Hinweis: Ein zu kleiner Wert kann verhindern, dass der Proxy antworten kann. Wenn eine Fehlermeldung des Proxys größer ist als die maximale Größe einer Antwort, erscheint keine Meldung bei einem Fehler. Aus diesem Grund werden Einträge, die kleiner als 10 kByte sind, auf 10 kByte gesetzt.

Aktivitäten in Logdatei aufzeichnen Wird diese Option aktiviert, werden alle Zugriffe in einer Logdatei protokolliert. In diesen Logdateien werden Datum, Uhrzeit, IP-Nummer des Clients und die aufgerufene URL gespeichert. Ist die Benutzerauthentifizierung eingeschaltet, steht auch der Benutzername in der Logdatei.
Hinweis: Dabei handelt es sich um nutzerbezogene Daten, die gesetzlichen Bestimmungen und dem Datenschutz unterliegen können. Es ist möglich, dass geltende Gesetze die Protokollierung untersagen, so dass sie deaktiviert bleiben muss.

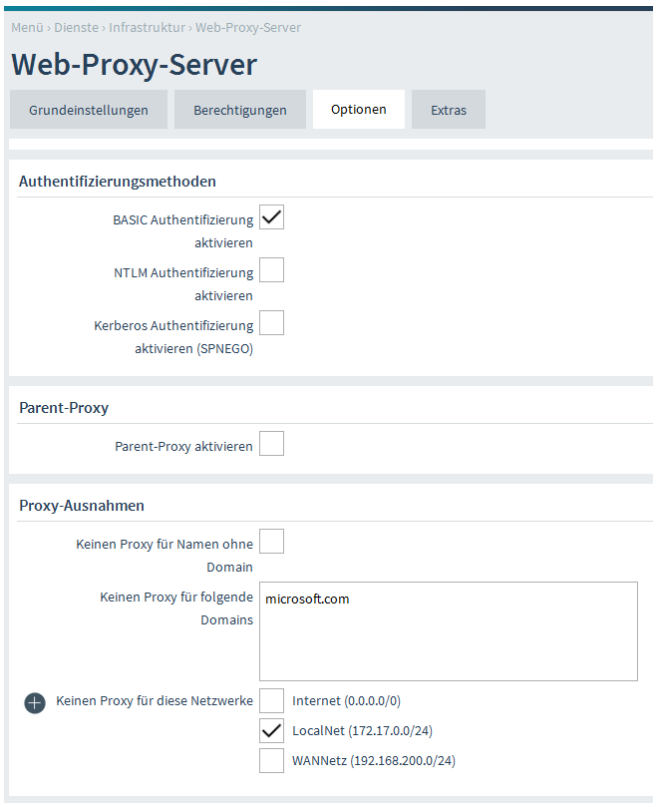
Logauswertung aktivieren Wird diese Option aktiviert, wird aus den Logdateien eine statistische Auswertung aufbereitet. Diese ist anonymisiert, d. h., es ist keine konkrete Zuordnung von URLs auf Nutzer möglich. Sehr wohl gibt es eine Aufschlüsselung des gesamten Traffics eines Nutzers oder eines Systems.

HTTP-Header anonymisieren Durch das Aktivieren dieser Option entfernt der Proxy bestimmte HTTP-Header aus den Anfragen, die er nach außen weiterreicht.

Anzahl der Redirector-Programme Hier wird die Anzahl der Prozesse angegeben, die der Webproxy zur Verarbeitung von URL-Anfragen startet. Das Redirect-Programm wird mehrfach gestartet, damit die eingehenden URLs zeitgleich abgearbeitet werden können. Die Anzahl kann erhöht werden, falls Anfragen verzögert abgearbeitet werden.

Entsprechende Logmeldungen können mit der Angabe Programm „squid“ unter *„Status/Wartung → Status → System → System-Logdateien“* eingesehen werden. Beispiel:

Consider increasing the number of redirector processes to at least ## in your config file.



BASIC Authentifizierung aktivieren Die einfachste Methode zur Authentifizierung von Benutzern ist die BASIC-Methode. Hiermit werden über ein Pop-Up des Web-Browsers die Benutzerinformationen abgefragt, wenn ein Benutzer über den Web-Proxy Internetseiten aufrufen will. An der Arbeitsstation sind keine weiteren Einstellungen erforderlich.

NTLM Authentifizierung aktivieren Diese Methode funktioniert nur, wenn der SMB/CIFS-Dienst aktiviert ist und kann verwendet werden, um Single-Sign-On mit älteren Betriebssystemen und Web-Browser zu bewerkstelligen. Entsprechende Arbeitsstationen müssen einer NT-Domäne oder AD beigetreten sein (gilt nicht für Windows Server 2008).

Kerberos Authentifizierung aktivieren (SPNEGO) Diese Methode ermöglicht es Windows-, Linux-, und Mac OS-Benutzern per Single-Sign-on in einem Kerberos-Realm am Web-Proxy anzumelden. Windows-Arbeitsstationen innnerhalb eines Active-Directory werden mit dieser Methode automatisch per Single-Sign-On authentifiziert.

Parent-Proxy aktivieren Mit dieser Option wird die Nutzung eines Parent-Proxy eingeschaltet. Proxyserver können „in Reihe“ geschaltet werden. Der Client schickt die Anfrage an seinem Proxy im lokalen Netz und dieser Proxy fragt wiederum einen weiteren Proxyserver, etwa beim Provider. Der Parent-Proxy ist solch ein übergeordnetes System.

Im letzten Abschnitt werden Netzwerke und Domains angegeben, für die der Proxy nicht verwendet werden soll.

Browser mit JavaScript-Unterstützung können automatisch für die Verwendung eines Proxys konfiguriert werden. Dazu muss in der Konfiguration des Browsers die URL einer JavaScript-Datei angegeben werden. Mit den Einstellungen in diesem Abschnitt wird die Konfigurationsdatei „proxy.pac“ erstellt und im Verzeichnis des Webservers abgelegt.

Keinen Proxy für Namen ohne Domain Wird diese Option aktiviert, wird kein Proxy verwendet, wenn keine Domain im Hostnamen enthalten ist, wenn also ein Server in der lokalen Domain angesprochen wird.

Keinen Proxy für folgende Domains Hier kann eine Liste von Domains angegeben werden, für die kein Proxy verwendet werden soll. Die Liste der Domains wird mit Leerzeichen getrennt.

Keinen Proxy für diese Netzwerke Hier können die Netzwerke ausgewählt werden, für die kein Proxy verwendet werden soll.

Regeln

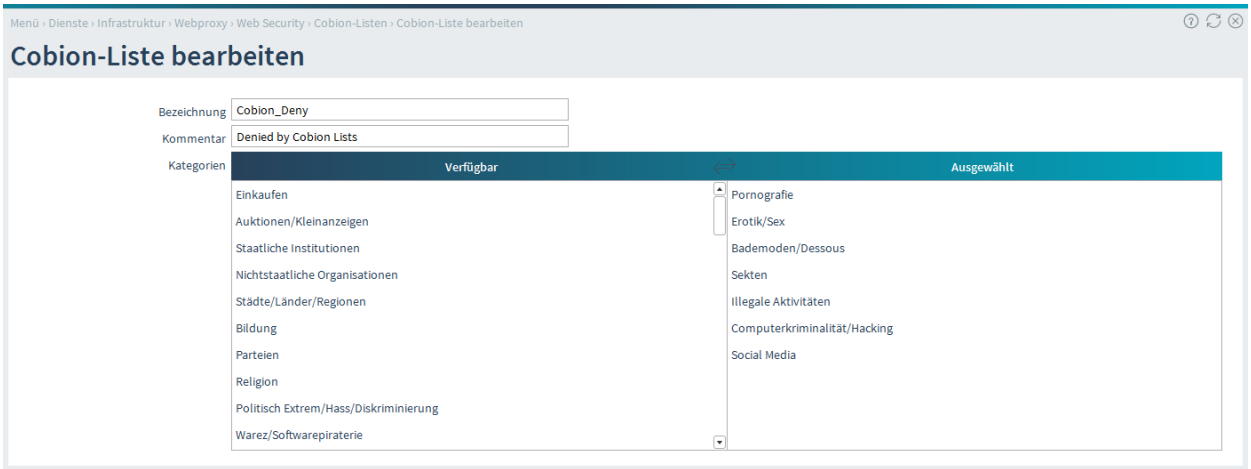
Dieser Dialog befindet sich unter *„Dienste → Infrastruktur →Web-Proxy →Web Security → Regeln“*

In diesem Dialog werden die Filterregeln für den Webproxyserver festgelegt. Eine solche Regel legt fest, welche URL-Listen zu welchen Zeiten gültig sind und ob die enthaltenen URLs gesperrt oder erlaubt werden.

In den Benutzungsrichtlinien kann festgelegt werden, für welche Gruppen die Regeln gültig sind. Dabei können für eine Gruppe auch mehrere Regeln gelten.

Die Reihenfolge der Regeln ergibt sich aus unterschiedlichen Prioritäten. Treffen mehrere Regeln auf eine URL zu, wird die mit der höchsten Priorität verwendet. Grundsätzlich sollte festgelegt werden, ob alles erlaubt wird und nur bestimmte URLs gesperrt werden oder ob alles gesperrt ist und nur bestimmte URLs erlaubt werden. Diese „Policy“ sollte in der vorhandenen „All-Regel“ eingestellt werden und die „All-Regel“ sollte ganz unten mit niedrigster Priorität angeordnet werden.

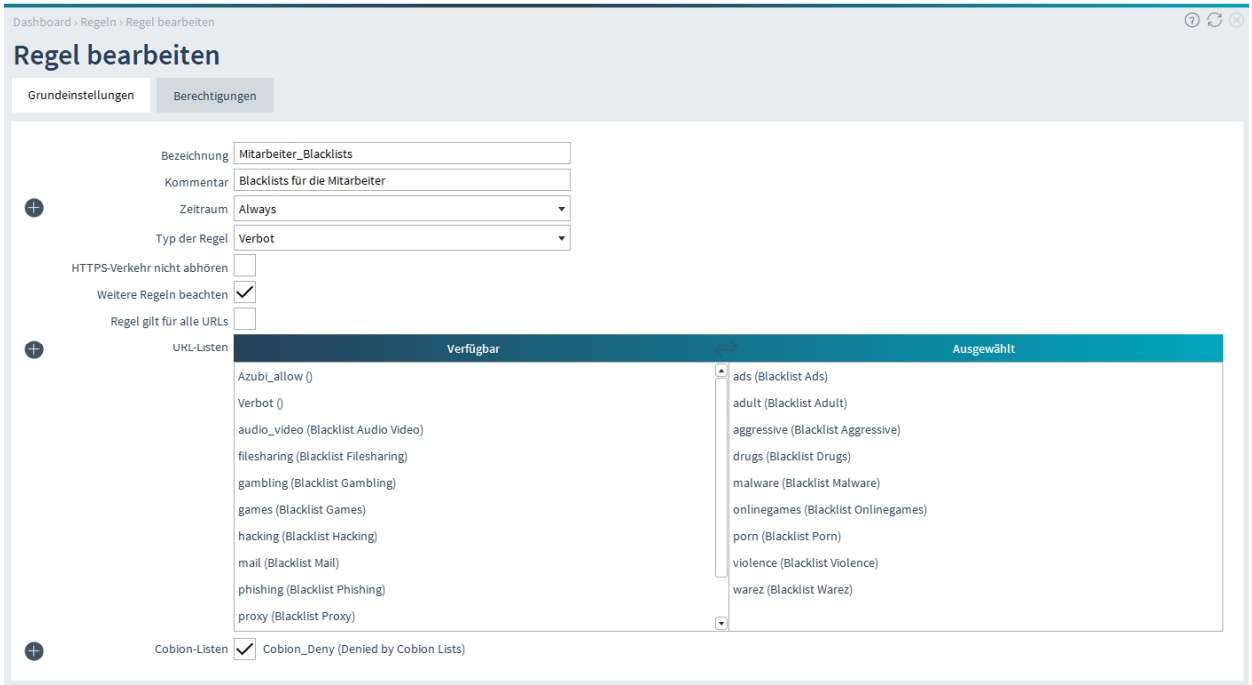
Um dem Administrator die Konfiguration der Regeln zu erleichtern, werden die *Collax Surf Protection* sowie die *Dansguardian Listen* eingesetzt. Hier sind viele URLs thematisch zu Gruppen zusammengefasst. Der Administrator kann die Kategorien auswählen, die für die Mitarbeiter verboten sein sollen. Um die *Collax Surf Protection* zu aktivieren benötigen Sie einen Lizenzschlüssel der über Collax bezogen werden kann. Erstellen Sie nach der Aktivierung Ihre individuellen *Cobion-Listen* unter *„Dienste → Infrastruktur →Web-Proxy →Web Security → Cobion-Listen“*



Um die *Dansguardian Listen* zu nutzen, installieren wir diese im Bereich *„Status/Wartung → Software → Lizenzen und Module“*. Klicken Sie zum Installieren auf das Plus hinter *„Dansguardian“.*

Für die Auszubildenden definieren wir noch eine *„Eigene Liste“* mit den beiden URLs *"collax.com" und "wikipedia.org"* unter *„Dienste → Infrastruktur →Web-Proxy →Web Security → Eigene Listen“*

Nun erstellen wir die gewünschten Regeln unter *„Dienste →Infrastruktur →Web-Proxy →Web Security →Regeln“*. Dafür sollten sprechende Namen verwendet werden. Über den Reiter *„Berechtigungen“* können die Gruppen ausgewählt werden, für die diese Regel gelten soll. Führen Sie diesen Schritt für jede definierte Proxy-Gruppe durch.



In der Übersicht sieht man die Regelliste, sortiert nach Priorität.

Prior...	Weitere Regeln beachten	Zweck	Bezeichnung	Kommentar
1	✓	Erlaubnis	Azubi_Erlaubnis	Nur die Whitelist ist für Azubis erlaubt
2	✗	Verbot	Azubis_Verboten	Alles andere ist verboten
3	✓	Erlaubnis	Mitarbeiter_Whitelist	explizite Whitelist für die Mitarbeiter
4	✓	Verbot	Mitarbeiter_Blacklists	Blacklists für die Mitarbeiter
5	✗	Erlaubnis	Mitarbeiter_Erlaubnis	Alles andere ist erlaubt
6	✗	Erlaubnis	GS_Alles_Arlaubt	Alles erlaubt

Es ist zu beachten, dass pro Gruppe (Ausnahme ist in unserem Fall die Gruppe Proxy_GL) immer mindestens eine Regel erstellt ist, die Restriktionen vorgibt (Priorität 2, 4 und 5). Abschließend (pro Gruppe) gibt es dann eine globale Regel (3, 6 und 7), die entweder alles erlaubt, oder alles verbietet. Die Regeln sollten immer so erstellt werden (bzw. wenn sie nachträglich erstellt wurden so verschoben werden), dass zuerst alle Regeln für die erste Gruppe, dann alle Regeln für die zweite Gruppe usw. untereinander stehen. Die Regeln oberhalb der abschließenden globalen Regel müssen immer das Feld *„Weitere Regeln beachten“* auf *„ja“* gesetzt haben.

Nehmen wir als Beispiel die Regeln für die Mitarbeiter.

1. Regel 4 enthält die *Whitelist* mit den Domains die, immer erlaubt sein sollen. z.B. die Homepage. Da weitere Regeln für diese Gruppe folgen setzen wir den Haken bei *„weitere Regeln beachten“*.
2. Regel 5 enthält die *Dansguardian- und Cobionlisten*, die für die Mitarbeiter immer verboten sein sollen. Auch hier gilt *„weitere Regeln beachten“*.
3. Regel 6: Abschliessende globale Regel. Diese Regel gilt für *„alle Domains“* und erlaubt den Zugriff auf die Seiten die durch die vorhergehenden nicht verboten wurden. Hier müssen dann für diese Gruppe keine weiteren Regeln beachtet werden.

Zugriffsmeldung

Eine typische Meldung einer Seite, deren Zugriff verboten ist, sieht folgendermaßen aus:

Virenschutz

Für die *Collax Virus Protetction und Avira AntiVir Protection* muss zunächst eine Lizenz erworben werden.

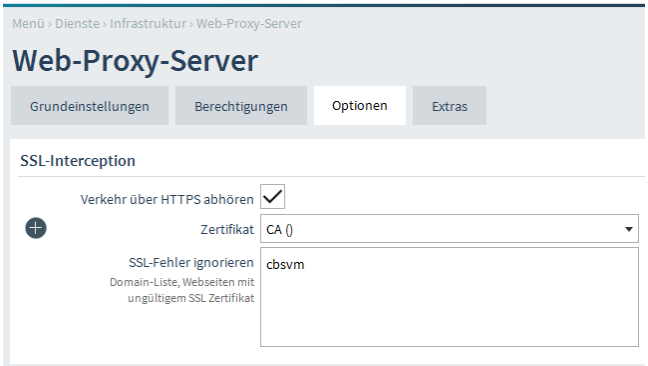
Installiert wird die Software über *„Status/Wartung → Software → Lizenzen und Module“*.

Darüberhinaus steht einem der kostenfreie Webfilter von ClamAV zur Verfügung.

Der Virenschutz muss nun lediglich unter *„System → Infrastruktur → Webproxy → Web Security → Antivirus Web-Filterung“* aktiviert werden und gilt dann automatisch für alle aufgerufenen HTTP Seiten, solange der Webproxy verwendet wird.

SSL-Interception

Dieser Dialog befindet sich unter *„Dienste → Infrastruktur → Web-Proxy → Web-Proxy-Server“* in den Optionen.



Der Inhalt von verschlüsseltem HTTP-Traffic (HTTPS) kann üblicherweise nicht bewertet oder gefiltert werden, da eine Verschlüsselung zwischen Web-Server und Browser stattfindet. In diesem Abschnitt können Einstellungen vorgenommen werden, die es dem Web-Proxy ermöglichen sich in diesen verschlüsselten Traffic einzuklinken, um den Inhalt auf z.B. auf schadhafte Software oder ungewollten Inhalt zu untersuchen.