

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 Security Gateway (CSG).

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 CSG.
2. Authentifizierung am Active Directory (AD) Server. Der Client meldet sich an der Windows Domäne an.

Der CSG 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.

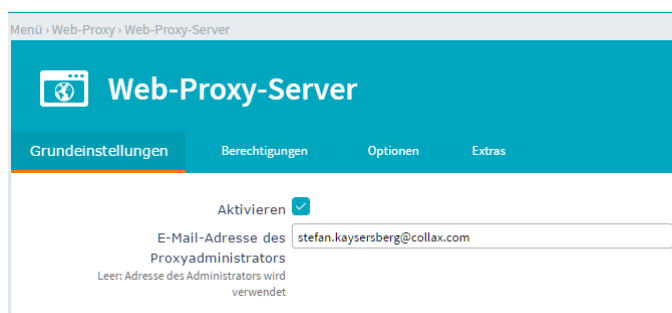
Zunächst werden 3 Gruppen angelegt:

- 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.

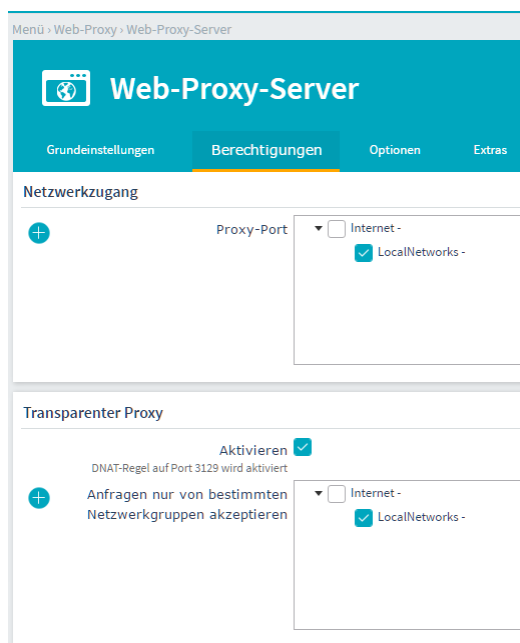
Wichtig: Jeder Benutzer muss daher einer dieser Gruppen zugeordnet sein.

Anschließend wird der Web-Proxy unter „Dienste → Web-Proxy → Web-Proxy-Server“ aktiviert und die Grundeinstellungen vorgenommen.



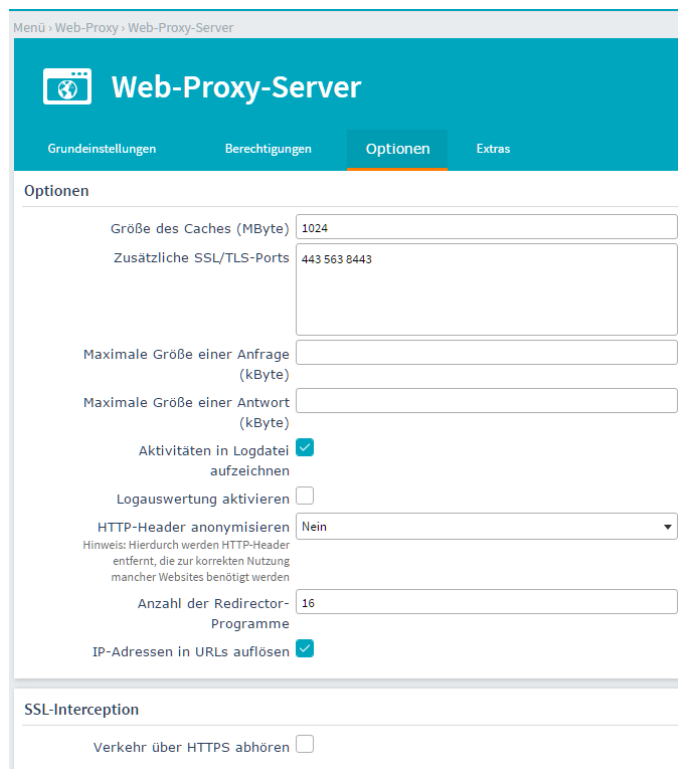
E-Mail-Adresse des Proxyadministrators Tritt ein Fehler auf, zeigt der Proxyserver eine Webseite mit einer Fehlermeldung an. Auf dieser Webseite wird die E-Mail-Adresse des lokalen Administrators angezeigt. Die Adresse wird in diesem Feld hinterlegt.

Unter *Berechtigungen* im Abschnitt *Netzwerkzugang* wird der Proxy-Port für die Netzwerkgruppen freigeschaltet. Der Port, auf dem der Proxy angesprochen wird, ist seitens des CSG fest auf 3128 eingestellt. Dies muss zusammen mit der IP-Adresse des Webproxy im Browser konfiguriert werden. Bei Verwendung eines transparenten Proxys ist im Browser keine spezielle Konfiguration erforderlich. Der transparente Proxy kann für den Dienst HTTP aktiviert werden. Datenpakete zum Zielport 80 werden dann von der Firewall „abgefangen“ und an den Webproxy umgeleitet.



Grundeinstellungen

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



The screenshot shows the 'Web-Proxy-Server' configuration page with the 'Optionen' tab selected. The settings are as follows:

- Größe des Caches (MByte): 1024
- Zusätzliche SSL/TLS-Ports: 443 563 8443
- Maximale Größe einer Anfrage (kByte): (empty)
- Maximale Größe einer Antwort (kByte): (empty)
- Aktivitäten in Logdatei aufzeichnen:
- Logauswertung aktivieren:
- HTTP-Header anonymisieren: Nein (dropdown menu)
- Anzahl der Redirector-Programme: 16
- IP-Adressen in URLs auflösen:

Below the 'Optionen' section is the 'SSL-Interception' section with the option 'Verkehr über HTTPS abhören' set to .

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 „System → Überwachung/Auswertung → Logdateien → System-Logdateien“ eingesehen werden. Beispiel:

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

IP-Adressen in URLs auflösen Die IP-Adressen werden dadurch in eine URL aufgelöst.

Verkehr über HTTPS abhören Um HTTPS-Traffic auf Inhalt oder auf schadhafte Software prüfen zu können, kann hier die Abhörfunktion eingeschaltet werden.

The screenshot shows the 'Web-Proxy-Server' configuration page with the 'Optionen' tab selected. The settings are as follows:

- Authentifizierungsmethoden:**
 - BASIC Authentifizierung aktivieren:
 - Kerberos Authentifizierung aktivieren (SPNEGO):
- Parent-Proxy:**
 - Parent-Proxy aktivieren:
- Proxy-Ausnahmen:**
 - Keinen Proxy für Namen ohne Domain:
 - Keinen Proxy für folgende Domains:
 - Keinen Proxy für diese Netzwerke:
 - Internet (0.0.0.0/0):
 - LocalNet (172.17.0.0/24):
 - Keinen Proxy für diese Hosts:
 - 0.collax.pool.ntp.org:
 - 1.collax.pool.ntp.org:

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.

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 innerhalb 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. Diese Einstellung kann automatisiert werden, indem im Browser bei der Proxy-Konfiguration ein automatisches Konfigurationsskript eingetragen wird. Dies ist nur vorhanden, wenn auf dem CBS neben dem Webproxy auch der Webserver aktiviert ist. Das Skript ist dann unter <http://CSG-Adresse/proxy.pac> abrufbar. Statt „CSG-Adresse“ muss entsprechend der Hostname oder die IP-Adresse des Collax Security Gateways verwendet werden.

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 → Web-Proxy → 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 → Web-Proxy → Cobion-Listen“

Menü » Web-Proxy » Cobion-Listen » Cobion-Liste bearbeiten

Cobion-Liste bearbeiten

Bezeichnung:

Kommentar:

Kategorien

Verfügbar	Ausgewählt
Abtreibung	Bademoden/Dessous
Aktienhandel/Börse	Computerkriminalität/Hacking
Alkohol	Erotik/Sex
Allgemeine Geschäftstätigkeiten	Illegale Aktivitäten
Anonyme Proxies	Pornografie
Architektur/Baugewerbe/Mobiliar	Sekten
Auktionen/Kleinanzeigen	Social Media
Bankwesen	
Bannerwerbung	
Belletristik/Bücher	

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

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

Menü » Web-Proxy » Eigene Listen » URL-Liste bearbeiten

URL-Liste bearbeiten

Name:

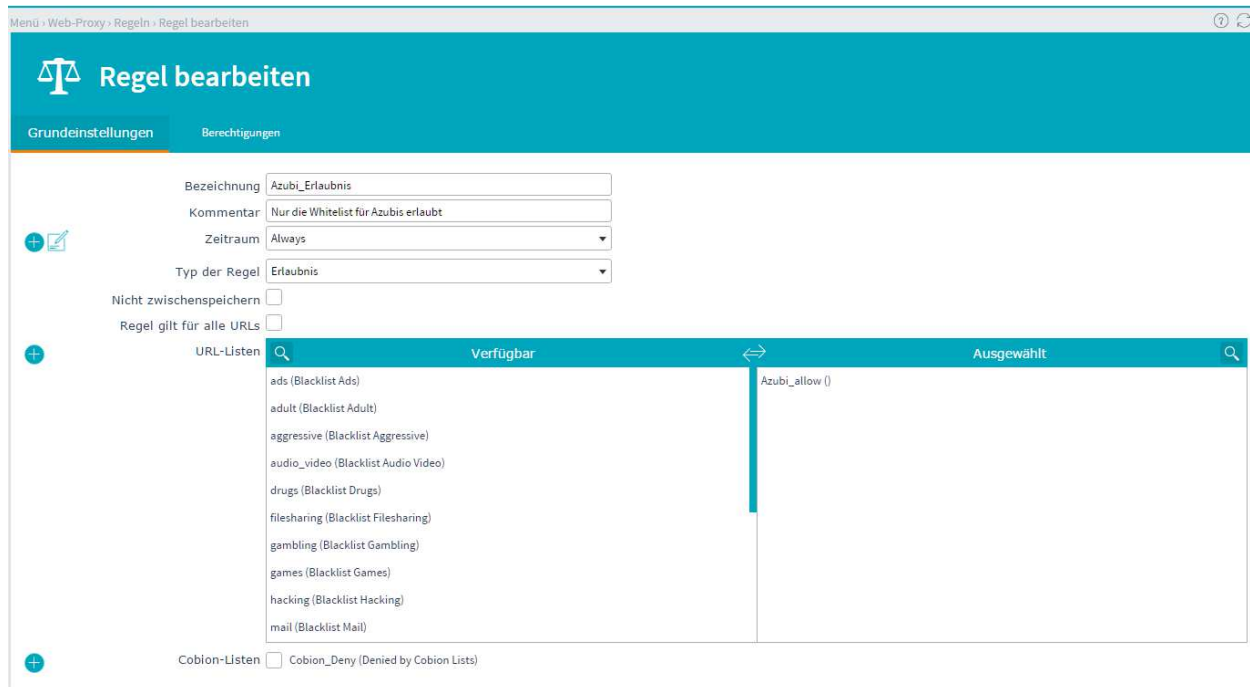
Kommentar:

URLs und Domains
durch Zeilenumbrüche getrennt:

Ausdrücke
durch Zeilenumbrüche getrennt:

URL-Datei hochladen:

Nun erstellen wir die gewünschten Regeln unter „Dienste → Web-Proxy → Regeln“. Dafür sollten sprechende Namen verwendet werden.



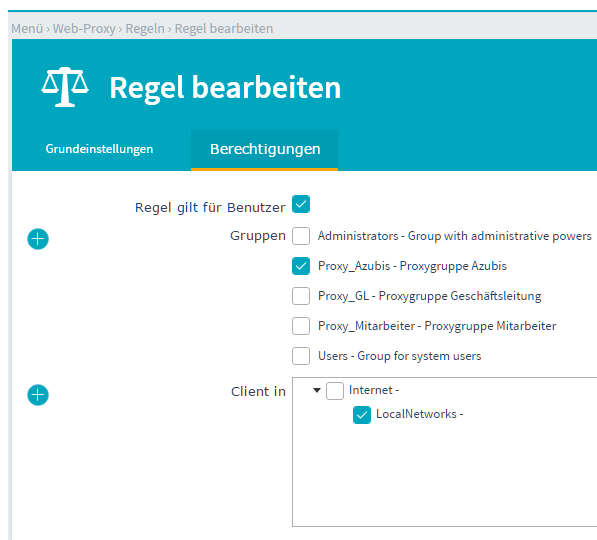
Zeitraum Hier muss der Zeitraum ausgewählt werden, zu dem die Regel gültig ist. Wird das Feld leergelassen, gilt die Regel zu jeder Zeit.

Typ der Regel Hier wird festgelegt, ob die Regel eine *Erlaubnis*, ein *Verbot* oder eine *Preload*-Regel ist.

URL-Listen Hier sollten die Listen aktiviert werden, auf die sich die Regel bezieht. Diese Liste ist nur sichtbar, wenn die Option Alle URLs nicht aktiviert ist.

Cobion-Listen In dieser Übersicht sind die Listen aus dem Cobion-Filter sichtbar und können ausgewählt werden.

Über den Reiter „*Berechtigungen*“ können die Gruppen ausgewählt werden, für deren Benutzer diese Regel gelten soll. Führen Sie diesen Schritt für jede definierte Proxy-Gruppe durch.



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

Menü > Web-Proxy > Regeln

Priori...	Bezeichnung	Kommentar	Zeitraum	Gilt für	Typ der Regel
1	Azubi_Erlaubnis	Nur die Whitelist für Azubis erlaubt	Always		Erlaubnis
2	Azubis_Verboten	Alles andere ist verboten	Always		Verbot
3	Mitarbeiter_Whitelist	explizite Whitelist für die Mitarbeiter	Always		Erlaubnis
4	Mitarbeiter_Blacklist	Blacklists für die Mitarbeiter	Always		Verbot
5	Mitarbeiter_Erlaubnis	Alles andere ist erlaubt	Always		Erlaubnis
6	GS_Alles_erlaubt	Alles erlaubt	Always		Erlaubnis

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 und 4). Abschließend (pro Gruppe) gibt es dann eine globale Regel (2, 5 und 6), 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.

Nehmen wir als Beispiel die Regeln für die Mitarbeiter.

1. Regel 3 enthält die *Whitelist* mit den Domains die, immer erlaubt sein sollen. z.B. die Homepage.
2. Regel 4 enthält die *Dansguardian- und Cobionlisten*, die für die Mitarbeiter immer verboten sein sollen
3. Regel 5: Abschliessende globale Regel. Diese Regel gilt für „alle Domains“ und erlaubt den Zugriff auf die Seiten die durch die vorhergehenden nicht verboten wurden.

Zugriffsmeldung

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



FEHLER
Die angeforderte URL konnte nicht gefunden werden

Der folgende Fehler wurde beim Versuch die URL <http://www.tagesschau.de/> zu holen festgestellt:

Zugriff verweigert.
(Alles andere ist verboten)

Die Anfrage wurde aufgrund mangelnder Zugriffsrechte verweigert. Bitte kontaktieren Sie Ihren Dienstanbieter falls sie denken, dass dies ein Fehler ist.

Ihr Cache Administrator ist stefan.kaysersberg@collax.com

Virenschutz

Für die *Collax Virus Protection* 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 „Dienste → Web-Proxy → Antivirus Web-Filterung“ aktiviert werden und gilt dann automatisch für alle aufgerufenen HTTP Seiten, solange der Webproxy verwendet wird.