

Web-Proxy für UCS

Thema:	Einführung, Installation und Konfiguration des Web-Proxy unter UCS
Datum:	15. Dezember 2009
Seitenzahl:	16
Versionsnummer:	4532
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Einführung	3
2	Installation des Proxy-Dienstes	3
3	Caching von Webinhalten	3
4	Protokollierung von Zugriffen	4
5	Einschränkung des Zugriffs auf erlaubte Netzwerke	4
6	Kaskadierung von Proxys	5
7	Benutzer-Authentifizierung am Proxy	5
8	Betrieb als transparenter Proxy	6
9	Konfiguration der verwendeten Ports	7
9.1	Zugriffs-Port	7
9.2	Erlaubte Ports	7
10	Filterung von Webinhalten mit univention-antivir-web	8
10.1	Installation	8
10.2	Filtern von Inhalten	8
10.3	Virenschanner	10
10.4	Eigene Dansguardian-Anpassungen	12
11	Konfiguration von Anwendungsprogrammen	12
11.1	Firefox	12
11.2	KDE-Programme	12
11.3	Internet Explorer	13
11.4	Kommandozeilen-Tools	13
11.5	Paketverwaltung	14

1 Einführung

Die UCS-Komponente **Web-Proxy** ermöglicht die Verwendung eines Web-Caches zur Verbesserung der Performance und Kontrolle des Datenverkehrs. Sie basiert auf dem bewährten Proxy-Server **Squid** und unterstützt die Protokolle HTTP, FTP und HTTPS.

Ein Proxy-Server nimmt Anfragen nach Internetinhalten entgegen und prüft, ob diese Inhalte bereits in einem lokalen Cache vorhanden sind. Ist dies der Fall, werden die angefragten Daten aus dem lokalen Cache bereitgestellt. Sind die Daten noch nicht vorhanden, werden die Inhalte vom jeweiligen Webserver abgerufen und in den lokalen Cache eingefügt. Hierdurch können die Antwortzeiten für die Anwender sowie das Transfervolumen über den Internetzugang verringert werden.

Als zusätzliche Komponente kann **univention-antivir-web** installiert werden. Damit ist es möglich, dass Internetinhalte vor Auslieferung an den Anwender überprüft und gefiltert werden, um so Dateien auf Viren zu scannen oder den Zugriff auf unerwünschte Inhalte zu unterbinden. Als zugrundeliegende Software wird hierbei **dansguardian** verwendet.

2 Installation des Proxy-Dienstes

Der Web-Proxy kann auf jeder UCS Server-Systemrolle installiert werden. Die Installation des Proxys kann dabei entweder im Rahmen der Installation oder nachträglich per Univention Management Console durch die Installation des Paketes **univention-squid** erfolgen. Der Dienst wird mit für den Betrieb ausreichenden Standardeinstellungen konfiguriert, sodass eine sofortige Verwendung möglich ist. Der Port, auf dem der Dienst erreichbar ist, kann nach eigenen Wünschen konfiguriert werden (siehe Kapitel 9.1), vorinstalliert ist Port 3128.

Werden Änderungen an der Konfiguration vorgenommen, muss **Squid** nach diesen Änderungen neu gestartet werden. Dies kann entweder über die Univention Management Console oder auf der Kommandozeile erfolgen:

```
/etc/init.d/squid restart
```

3 Caching von Webinhalten

Squid ist ein **CachingProxy**, d.h. zuvor schon einmal angefragte Inhalten können aus einem Cache zur Verfügung gestellt werden ohne erneut vom jeweiligen Webserver geladen zu werden. Dies kann in einigen Umgebung zur schnelleren Bearbeitung von Webanfragen führen. Außerdem reduziert es den Datenverkehr, der über die externe Anbindung ausgetauscht wird.

In manchen Umgebung ist diese Caching-Funktionalität allerdings nicht notwendig bzw. muss bei kaskadierten Proxys nicht bei allen aktiviert sein. Für diese Szenarien kann

die Caching-Funktion des Squid mit der Univention Configuration Registry-Variable `squid/cache` deaktiviert werden, indem diese auf den Wert **no** gesetzt wird. Anschließend muss der Squid neugestartet werden.

4 Protokollierung von Zugriffen

Sämtliche Zugriffe, die über den Proxy-Server vorgenommen werden, werden in einer Logdatei erfasst. Anhand dieser Logdatei ist es möglich, nachzuvollziehen auf welche Webseiten zugegriffen wurde. Die Logdatei befindet sich unter [/var/log/squid/access.log](#).

Es ist auch möglich, die Logdateien mit zusätzlichen Programmen aufzubereiten und Berichte zu erstellen. Dies ist z.B. mit **srg** oder **modlogan** machbar (beide noch nicht im Lieferumfang von UCS enthalten).

Bei Verwendung von **univention-antivir-web** werden sämtliche Zugriffe in der Datei [/var/log/dansguardian/access.log](#) protokolliert.

5 Einschränkung des Zugriffs auf erlaubte Netzwerke

Standardmäßig darf nur aus lokalen Netzwerken auf den Proxy-Server zugegriffen werden. Ist z.B. an dem Rechner, auf dem Squid installiert wurde, ein Netzwerkinterface mit der Adresse 192.168.1.10 und der Netzmaske 255.255.255.0 vorhanden, dürfen nur Rechner aus dem Netzwerk 192.168.1.0/24 auf den Proxy-Server zugreifen. Weitere Netzwerke können über die Univention Configuration Registry-Variable `squid/allowfrom` angegeben werden. Dabei muss die CIDR-Notation verwendet werden, mehrere Netzwerke sind durch Leerzeichen zu trennen.

Beispiel:

```
univention-config-registry set squid/allowfrom="192.168.2.0/24 192.168.3.0/24"
```

Nach einem Neustart von Squid ist jetzt der Zugriff aus den Netzwerken 192.168.1.0/24, 192.168.2.0/24 und 192.168.3.0/24 erlaubt.

Wenn Squid zusammen mit Dansguardian eingesetzt wird, d.h. die Viren- oder Webinhaltsfilterung aktiviert wird, kann Squid den Zugriff nicht prüfen, da die Verbindungen über Dansguardian erfolgen. In diesem Fall kann der Zugriff über Dansguardian eingeschränkt werden.

Dafür muss die Univention Configuration Registry-Variable `dansguardian/auth/ip` auf den Wert **yes** gesetzt werden, wodurch für Dansguardian die Authentifizierung anhand der Client-IP-Adressen aktiviert wird. Mit diesem Modul können verschiedene Gruppen von Netzwerken mit zugehörigen Zugriffsregeln definiert werden. Somit kann für Netzwerke entweder der Zugriff komplett gesperrt oder aber einige bzw. alle Zugriffe erlaubt werden.

In folgendem Beispiel wird der Zugriff für das Netzwerk 192.168.0.0/24 und die IP-Adresse 192.168.0.46 gesperrt und für alle anderen erlaubt.

Beispiel:

```
univention-config-registry set dansguardian/groups=gesperrt;frei
univention-config-registry set dansguardian/groups/gesperrt/banned/sites=**
univention-config-registry set dansguardian/groups/gesperrt/addresses=\
    192.168.0.46;192.168.1.0/255.255.255.0
```

6 Kaskadierung von Proxys

In einigen Szenarien kann eine Kaskadierung von Proxy-Servern gewünscht sein. Hierbei greifen einzelne Proxy-Server beim Abruf von Internetseiten wiederum auf logisch über ihnen gelegene Proxy-Server zurück, die dann die angeforderten Daten aus dem Internet beziehen. Hierdurch kann eine hierarchische Struktur von Proxy-Servern erreicht werden und z.B. in einer Firmenzentrale ein Haupt-Cache betreiben werden, auf den die Proxy-Server an den einzelnen Standorten zurückgreifen.

Der jeweils übergeordnete Proxy-Server wird hierbei als **Parent Proxy** bezeichnet. Der Parent Proxy kann über die Univention Configuration Registry-Variablen `squid/parent/host` (IP-Adresse oder Rechnername) und `squid/parent/port` (Portnummer) festgelegt werden.

Anfragen an Rechner im lokalen Netzwerk des Proxy-Servers werden direkt beantwortet und nicht an den Parent Proxy weitergeleitet. Sollen weitere Netzwerke von der Weiterleitung an den Parent Proxy ausgenommen werden, können diese über die Univention Configuration Registry-Variable `squid/parent/directnetworks` festgelegt werden. Dabei muss die CIDR-Notation verwendet werden, mehrere Netzwerke sind durch Leerzeichen zu trennen.

Beispiel:

```
univention-config-registry set squid/parent/directnetworks=192.168.2.0/24
```

Hierdurch werden Anfragen, die an Webserver im lokalen Netzwerk oder im Netzwerk 192.168.2.0/24 gestellt werden, vom Proxy-Server nicht an den Parent-Proxy weitergeleitet, sondern direkt beantwortet.

7 Benutzer-Authentifizierung am Proxy

Oftmals ist es notwendig, dass nur bestimmte Benutzer Zugriff auf Webseiten erhalten sollen. Squid ermöglicht die benutzerbezogene Zugriffsregelung über Gruppenmitgliedschaften. Dadurch wird erreicht, dass nur Mitglieder bestimmter Benutzergruppen den Proxy benutzen dürfen. Um eine Überprüfung der Gruppenmitgliedschaft zu ermöglichen,

ist es hierbei erforderlich, dass eine Anmeldung des Benutzers am Proxy-Server durchgeführt wird.

Achtung:

Um zu verhindern, dass nicht autorisierte Benutzer trotzdem Internetseiten abrufen können, sind weitere Maßnahmen erforderlich, damit diese Benutzer nicht am Proxy-Server vorbei auf das Internet zugreifen können. Dies kann z.B. erreicht werden, indem auf einem Router nur Webseiten-Anfragen weitergeleitet werden, die vom Proxy-Server kommen.

Die Authentifizierung und die damit erst mögliche Überprüfung der Gruppenzugehörigkeiten muss zuerst aktiviert werden. Dafür werden verschiedene Mechanismen angeboten: Sie kann entweder direkt gegen den LDAP-Server erfolgen oder eine NTLM-Authentisierung durchgeführt werden. Letztere bietet den Vorteil, dass beim Zugriff von Windows-Rechnern keine erneute Eingabe des Passworts notwendig ist.

Um die Authentisierung über LDAP zu aktivieren muss die Univention Configuration Registry-Variable `squid/ldapauth` und für NTLM die Univention Configuration Registry-Variable `squid/ntlmauth` auf den Wert **yes** gesetzt werden.

Die Benutzergruppen, die den Web-Proxy verwenden dürfen, können über die Univention Configuration Registry-Variable `squid/ldapauth/groups` (unabhängig von dem gewählten Mechanismus zur Authentifizierung) definiert werden. Ist die Variable nicht gesetzt, wird die Gruppe 'www-access' als Standard verwendet. Bei Angabe mehrerer Gruppen sind diese durch ein Semikolon zu trennen:

Beispiel:

```
univention-config-registry set squid/ldapauth/groups="squidusers;www-access"
```

Mit dieser Einstellung dürfen sich Mitglieder der Gruppen **squidusers** und **www-access** am Proxy-Server anmelden.

Achtung:

Die konfigurierten Gruppennamen dürfen keine Leerzeichen und keine Großbuchstaben enthalten. Soll einer solchen Gruppe der Zugriff auf den Proxy-Server trotzdem erlaubt werden, kann eine neue Gruppe angelegt und die gewünschte Gruppe als Mitglied dieser Gruppe konfiguriert werden

8 Betrieb als transparenter Proxy

Soll vermieden werden, dass in den Anwendungsprogrammen (z.B. im Webbrowser) der zu verwendende Proxyserver konfiguriert werden muss, gibt es die Möglichkeit, Squid als transparenten Proxy zu konfigurieren. Dadurch werden automatisch alle Web-Anfragen, die von einem Client abgeschickt werden, auf den Proxy-Server umgeleitet und von diesem beantwortet.

Voraussetzung für eine solche Konfiguration ist, dass der Proxy-Server auf allen Clients in der Netzwerkkonfiguration als Standardgateway eingetragen ist. Die LDAP-



Authentifizierung auf dem Proxy-Server darf dabei nicht aktiviert sein.

Durch Setzen der Univention Configuration Registry-Variable `squid/transparentproxy` auf **yes** werden in der Datei `/etc/security/netfilter.d/20squid` Paketfilterregeln eingetragen. Durch diese Regeln werden alle Anfragen, die über das UCS-System geleitet werden, auf den Proxy-Server umgeleitet. Es werden dabei Zugriffe auf die Netzwerk-Ports umgeleitet, auf die laut der Univention Configuration Registry-Variable `squid/webports` über den Proxy-Server zugegriffen werden darf (siehe unten).

Damit die Filterregeln aktiviert werden, muss die Paketfilter-Komponenten neu gestartet werden. Hierbei darf diese Komponente nicht über die Univention Configuration Registry-Variable `security/disabled` deaktiviert sein:

```
/etc/init.d/univention-iptables restart
```

9 Konfiguration der verwendeten Ports

9.1 Zugriffs-Port

Standardmäßig ist der Web-Proxy über den Port 3128 erreichbar. Ist ein anderer Port gewünscht, kann dieser über die Univention Configuration Registry-Variable `squid/httpport` konfiguriert werden.

Beim Einsatz des Inhalts- und Virenschanners (siehe Kapitel 10), der im nächsten Abschnitt beschrieben ist, ist dieser an Stelle von Squid unter dem konfigurierten Port erreichbar. Squid belegt dann den nächsthöheren Port. Dies sollte beachtet werden, wenn es weitere Anwendungen gibt, die auf diesem Port Dienste anbieten sollen.

9.2 Erlaubte Ports

In der Standardkonfiguration leitet Squid nur Anfragen von Clients weiter, die an die Netzwerkports 80 (HTTP), 443 (HTTPS) oder 21 (FTP) gerichtet werden. Die Liste der erlaubten Ports kann über die Univention Configuration Registry-Variable `squid/webports` geändert werden, mehrere Angaben sind dabei durch Leerzeichen zu trennen:

Beispiel:

```
univention-config-registry set squid/webports="80 443"
```

Durch diese Einstellung wird nur noch der Zugriff auf die Ports 80 und 443 (HTTP und HTTPS) erlaubt.

Ist der Betrieb als transparenter Proxy aktiviert, werden die IPTables-Regeln entsprechend angepasst. Damit die neuen Regeln verwendet werden, muss die Netzwerkfilter-Komponente (`/etc/init.d/univention-iptables`) neu gestartet werden. Weitere Hinweise dazu sind im UCS-Handbuch zu finden.

10 Filterung von Webinhalten mit univention-antivir-web

Um den Zugriff auf bestimmte Web-Inhalte zu sperren, kann die Komponente **univention-antivir-web** eingesetzt werden. Damit ist es möglich,

- bestimmte Dateiarten und -endungen für den Download zu sperren
- den Zugriff auf einzelne Webseiten zu unterbinden
- einzelnen Rechnern den Zugriff auf den Proxy-Server zu verbieten
- herunterzuladene Dateien auf Viren zu scannen
- einzelne Dateien oder Webseiten vom Virenscan auszunehmen

Für die Filterfunktionen wird die Software **Dansguardian** eingesetzt. Diese Software nimmt Webseiten-Anforderungen aus dem Netzwerk entgegen und prüft, ob Zugriffe des Absenders der Anfrage erlaubt sind. Falls ja, wird die Anfrage an den Proxy-Server Squid weitergeleitet.

Achtung:

Der direkte Zugriff auf den Proxy-Server Squid ist hierbei auf Zugriffe vom lokalen Rechner ('localhost') eingeschränkt. Anwender, die auf dem System arbeiten, auf dem Squid und Dansguardian installiert sind, haben so die Möglichkeit, die Filterfunktionen zu umgehen, indem Sie direkt auf Squid zugreifen. Der Web-Proxy und **univention-antivir-web** sollten deshalb nur auf dedizierten Systemen installiert werden, auf denen Anwender sich nicht anmelden können.



10.1 Installation

univention-antivir-web kann über das gleichnamige Paket installiert werden. Nach der Installation ist der Virens Scanner aktiviert, der Filter für Webinhalte ist nicht aktiv.

Das Filtern von Web-Inhalten und der Virens Scanner können getrennt voneinander aktiviert werden. Um den Inhaltsfilter zu aktivieren, muss die Univention Configuration Registry-Variable `squid/contentscan` auf **yes** gesetzt und Squid neu gestartet werden. Um den Virens Scanner zu verwenden, ist `squid/virusscan` auf **yes** zu setzen. Ist keine der beiden Variablen auf **yes** gesetzt, wird **univention-antivir-web** nicht verwendet.

10.2 Filtern von Inhalten

Webinhalte können anhand von Dateiendungen, MIME-Typen, Webseiten sowie einzelnen URLs gefiltert werden. Es ist dabei möglich, einzelne Rechner oder Nutzer aus der Filterung auszunehmen.

Die Filterfunktion kann über die folgenden Univention Configuration Registry-Variablen konfiguriert werden. Sollen dabei mehrere Werte angegeben werden, sind diese jeweils

durch Leerzeichen zu trennen. Die Filterung wird bei Dansguardian auf Basis von Gruppenzugehörigkeiten durchgeführt, d.h. es können pro Gruppe verschiedene Regeln definiert und dadurch verschiedene Berechtigungen beim Zugriff auf das Web realisiert werden. Welche Gruppen von Dansguardian betrachtet werden, wird in der Univention Configuration Registry-Variablen `dansguardian/groups` definiert.

```
univention-config-registry set dansguardian/groups=webgrp1;webgrp2
```

Dabei ist zu beachten, dass die erste Gruppe in der Liste eine besondere Rolle spielt. Alle Benutzer, die keiner der angegebenen Gruppen zugeordnet werden können, werden dieser zugeordnet, d.h. die definierten Filterregeln gelten. In der Regel wird dieser Gruppe somit die geringste Berechtigung zugeordnet.

Damit vorgenommene Änderungen aktiviert werden, muss Dansguardian mit

```
/etc/init.d/dansguardian restart
```

neu gestartet werden. Für die Änderungen von Filterregeln reicht es aus Dansguardian zum erneuten Laden der Konfiguration aufzufordern. Dies wird mit dem folgenden Kommando erwirkt:

```
dansguardian -g
```

Die Univention Configuration Registry-Variablen zur Definition der Filterregeln enthalten den Gruppennamen, welcher in der folgenden Liste durch **<group>** ersetzt wird.

<code>squid/contentscan</code>	Diese Variable muss auf yes gesetzt sein, damit Webinhalte gefiltert werden.
<code>dansguardian/<group>/banned/extensions</code>	Dateien mit den angegebenen Dateiendungen dürfen nicht heruntergeladen werden. Der Trennpunkt muss dabei mit angegeben werden. Ist diese Variable leer, werden Standardwerte verwendet. Um alle Dateiendungen zu erlauben, muss die Variable auf <code>' '</code> gesetzt werden (Zeichenkette mit einem Leerzeichen). Beispiel: <code>'.doc .xls .exe'</code>
<code>dansguardian/<group>/banned/mimetypes</code>	Dateien mit dem angegebenen MIME-Type dürfen nicht heruntergeladen werden. Der MIME-Type wird dabei vom ausliefernden Webserver (bzw. einer darauf laufenden Anwendung) festgelegt. Normalerweise sollten die zu den oben erläuterten Dateiendungen passenden MIME-Type angegeben werden. Ist diese Variable leer, werden Standardwerte verwendet. Um alle MIME-Type zu erlauben, muss die Variable auf <code>' '</code> gesetzt werden (Zeichenkette mit einem Leerzeichen). Beispiel: <code>"audio/mpeg application/zip"</code>
<code>dansguardian/<group>/banned/sites</code>	Hiermit können komplette Webauftritte gesperrt werden. Beispiel: <code>illegale-webseite.com</code>

dansguardian/<group>/banned/urls	Im Gegensatz zum vorherigen Parameter können hiermit einzelne Webseiten oder Teilbereiche von Webauftritten gesperrt werden. Um z.B. http://www.meineschule.de/bilder/ zu sperren, kann <code>www.meineschule.de/bilder/</code> verwendet werden.
dansguardian/<group>/banned/clientips	Diese Variable ermöglicht es, einzelne Rechner über die IP-Adresse komplett vom Zugriff auf den Proxy-Server auszuschließen. Beispiel: <code>192.168.1.17</code>
dansguardian/<group>/exception/ipaddresses	Hiermit können für einzelne Rechner sämtliche Filterfunktionen deaktiviert werden, sodass von diesem Rechner alle Dateien über den Proxy-Server heruntergeladen werden dürfen. Dies kann nützlich sein, wenn z.B. von einem Administrations-Rechner Dateien für weitere Benutzer heruntergeladen werden sollen. Beispiel: <code>192.168.1.7</code>
dansguardian/<group>/exception/user	Analog zur IP-Whitelist können hiermit einzelne Benutzer von der Filterfunktionalität ausgeschlossen werden. Damit dies funktioniert, muss die Anmeldung am Proxy-Server aktiviert worden sein.

Tabelle 1: Filtermöglichkeiten

10.3 Virenschanner

Angeforderte Dateien können, während Sie vom Proxy-Server heruntergeladen werden, auf Viren überprüft werden. Dabei kommt in der Standardeinstellung der freie Virenschanner **Clamav** zum Einsatz. Die Integration weiterer Virenschanner ist möglich.

Der Virenschanner kann über die folgenden Univention Configuration Registry-Variablen konfiguriert werden. Sollen dabei mehrere Werte angegeben werden, sind diese jeweils durch Leerzeichen zu trennen.

squid/virusscan	Diese Variable muss auf yes gesetzt sein, damit Webinhalte auf Viren gescannt werden.
-----------------	--

dansguardian/virusscanner	<p>Diese Variable definiert den zu verwendenden Virenschanner. In der Vorgabe ist diese Univention Configuration Registry-Variable auf den Wert clamav gesetzt. Für diesen Scanner ist auch eine Vorkonfiguration enthalten. Für alle weiteren Scanner, die zur Verfügung stellen muss die Konfiguration unterhalb von /etc/dansguardian/contentscanners/ angepasst werden. Mögliche weitere Scanner, die eingetragen werden können:</p> <p>clamdscan ClamAV im Daemon-Modus</p> <p>kavdscan Kaspersky Scanner</p> <p>icapscan ICAP AV Server</p> <p>commandlinescan Zur Einbindung beliebiger weiterer Virenschanner auf Basis von Kommandozeilentools</p>
dansguardian/virus/notifyemail	<p>Ist dieser Wert auf eine gültige E-Mail-Adresse gesetzt, erfolgt eine Benachrichtigung per E-Mail, sobald ein Benutzer versucht, eine mit einem Virus infizierte Datei herunterzuladen. Voraussetzung ist, dass das System, auf dem univention-antivir-web installiert ist, Mails versenden kann.</p>
dansguardian/virus/exception/extension	<p>Dateien, die über eine in dieser Variable angegebene Dateiendung verfügen, werden nicht auf Viren geprüft. Diese Option sollte vorsichtig eingesetzt werden, da Dateiendungen keine Aussage über den tatsächlichen Inhalt einer Datei erlauben.</p>
dansguardian/virus/exception/mimetypes	<p>In dieser Variable angegebenen MIME-Type werden nicht auf Viren gescannt. Auch diese Option sollte vorsichtig eingesetzt werden.</p>
dansguardian/virus/exception/sites	<p>Hiermit können komplette Webauftritte vom Scannen auf Viren ausgenommen werden. Beispiel: <code>partnerfirma.de</code></p>
dansguardian/virus/exception/urls	<p>Im Gegensatz zum vorherigen Parameter können hiermit einzelne Webseiten oder Teilbereiche von Webauftritten freigegeben werden. Um z.B. ftp://www.partnerfirma.de/bilanzen/ freizugeben, kann <code>www.partnerfirma.de/bilanzen/</code> verwendet werden.</p>

Tabelle 2: Konfigurationsmöglichkeiten für den Virenschanner

10.4 Eigene Dansguardian-Anpassungen

Dansguardian bietet Filtermöglichkeiten, die über die oben angegebenen Konfigurationseinstellungen hinaus gehen. Um entsprechende Filter zu konfigurieren, kann die Filterkonfiguration selber angepasst werden. Damit ist es z.B. möglich:

- Webseiten zu sperren, die bestimmte Wörter enthalten
- bestimmte Suchoptionen bei bekannten Suchmaschinen zu erzwingen
- Webseiten mit einem Scoring-Mechanismus zu bewerten und erst ab einem bestimmten Schwellwert die Seite zu sperren
- Web-Präsenzen komplett zu sperren, den Zugriff auf einzelne Abschnitte jedoch trotzdem zu erlauben

Die Konfigurationsdateien für Dansguardian befinden sich im Verzeichnis `/etc/dansguardian/`. Diese Dateien werden nicht über den Univention Configuration Registry-Mechanismus verwaltet, gewünschte Änderungen müssen deshalb in den Templates für diese Dateien vorgenommen werden. Weitere Hinweise hierzu finden sich im UCS-Handbuch.

11 Konfiguration von Anwendungsprogrammen

Sofern kein transparenter Web-Proxy konfiguriert wurde, muss die Verwendung des Proxy-Servers in den verschiedenen Anwendungsprogrammen einzeln aktiviert werden.

11.1 Firefox

Der Dialog für die Proxy-Konfiguration wird über **Bearbeiten → Einstellungen → Erweitert → Netzwerk → Einstellungen...** aufgerufen (siehe Abbildung 1).

Hier ist **Manuelle Proxy-Konfiguration** zu wählen und der zu verwendende Proxy-Server einzutragen. Üblicherweise kann **Für alle Protokolle diesen Proxy-Server verwenden** aktiviert werden.

11.2 KDE-Programme

Die Proxy-Einstellung für alle KDE-Programme (z.B. Konqueror) kann über das KDE-Kontrollzentrum vorgenommen werden. Das KDE-Kontrollzentrum kann entweder über den entsprechenden Menüeintrag im K-Menü oder durch Ausführen des Befehls `kcontrol` aufgerufen werden. Die Proxy-Konfiguration befindet sich unter **Internet & Netzwerk → Proxy**. Hier ist **Proxy-Einstellungen manuell vornehmen** zu aktivieren, über **Einrichtung...** lassen sich die Verbindungsdaten zum Proxy eingeben. Auch hier sollte **Für alle Protokolle den selben Proxy-Server verwenden** aktiviert werden (siehe Abbildung 2).

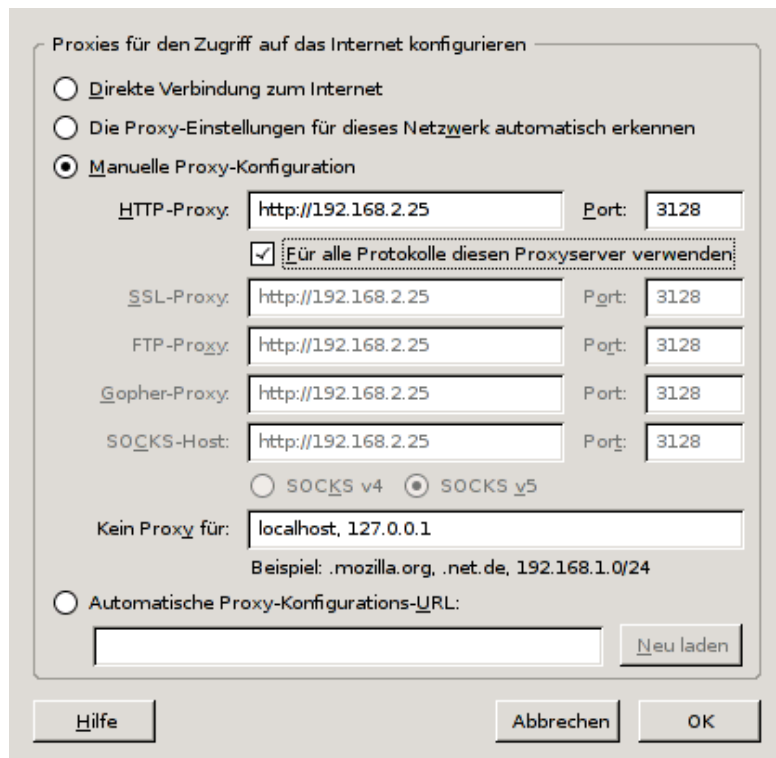


Abbildung 1: Proxy-Konfiguration in Firefox

11.3 Internet Explorer

Die Proxy-Einstellungen für den Internet Explorer lassen sich in den Internet-Optionen eintragen, die je nach verwendeter Windows-Version auf verschiedene Arten aufgerufen werden. In den Internet-Optionen ist **Verbindungen** → **LAN-Einstellungen** aufzurufen und in dem sich öffnenden Fenster die Verbindungsdaten zum Proxy einzutragen (siehe Abbildung 3).

11.4 Kommandozeilen-Tools

Die meisten Kommandozeilen-Tools, die Zugriffe auf Webserver durchführen (z.B. `wget`, `lynx` oder `curl`), prüfen, ob die Umgebungsvariable `http_proxy` gesetzt ist. Ist dies der Fall, wird automatisch der in dieser Variable eingestellte Proxy-Server verwendet. Die Univention-Befehle zur Systemverwaltung prüfen ebenfalls auf diese Variable.

Über die Univention Configuration Registry-Variable `proxy/http` kann das Setzen dieser Umgebungsvariable durch einen Eintrag in `/etc/profile` aktiviert werden. Dabei ist zu beachten, dass die u.a. Univention-spezifischen Paketverwaltungsprogramme normalerweise auf den den Repository-Server über den DNS-Alias ***univention-repository*** zugrei-

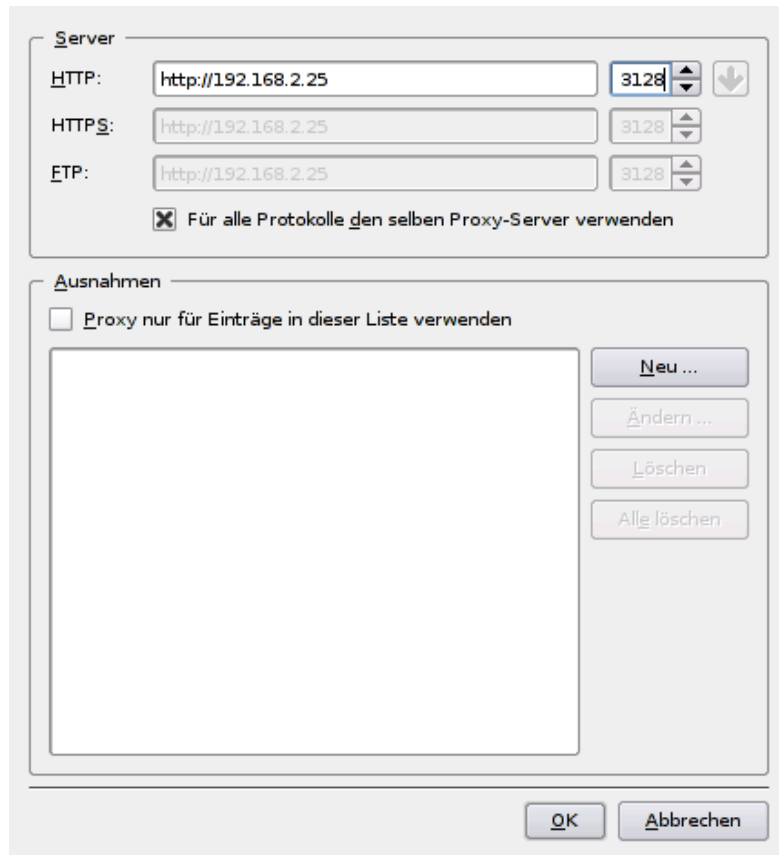


Abbildung 2: Proxy-Konfiguration für KDE

fen. Der verwendete Proxy muss diesen DNS-Alias korrekt auflösen können.

Beispiel:

```
univention-config-registry set proxy/http=http://192.168.2.25
```

Achtung:

Diese Änderung wird nicht für aktuell geöffnete Sitzungen übernommen. Damit die Änderung aktiv wird, muss ein neuer Login erfolgen.



11.5 Paketverwaltung

Die UCS-Programme zur Paketverwaltung sowie das Debian-Paketverwaltungsprogramm **apt** bieten ebenfalls Unterstützung für den Download von Paketen über einen Proxy-Server. Hierzu ist es ausreichend, die Univention Configuration Registry-Variable

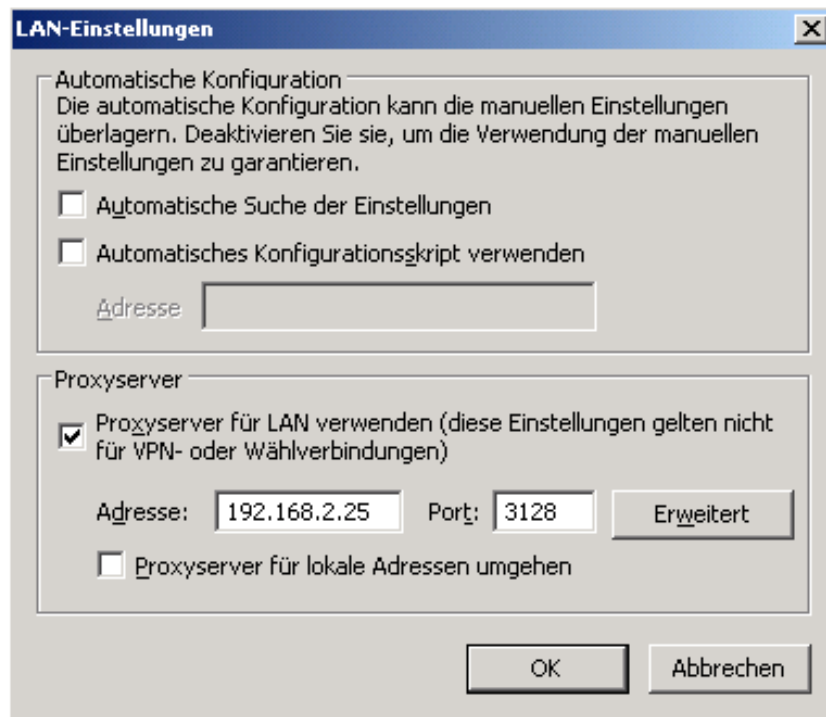


Abbildung 3: Proxy-Konfiguration für den Internet Explorer

proxy/http entsprechend zu setzen (siehe oben). Darüber hinaus gibt es teilweise noch weitere Möglichkeiten, die Verwendung eines Proxys zu konfigurieren.

11.5.1 apt

apt wird (unter anderem von **univention-actualise**) für die Installation einzelner Pakete aufgerufen und lädt die angeforderten Programme gemäß den Einträgen in `/etc/apt/sources.list` herunter (dort ist üblicherweise der UCS Repository-Server eingetragen). Neben der Konfiguration des Proxy-Servers über die Univention Configuration Registry-Variable `proxy/http` kann hier zusätzlich der zu verwendende Benutzername und ein Passwort in den Univention Configuration Registry-Variablen `proxy/username` und `proxy/password` konfiguriert werden.

Achtung:

Das hier angegebene Passwort wird in die Datei `/etc/univention/base.conf` geschrieben, die von jedem gelesen werden darf.



Die Proxy-Konfiguration befindet sich in `/etc/apt/apt.conf.d/80proxy` und wird über ein

Univention Configuration Registry-Template verwaltet, an dem gewünschte Änderungen vorgenommen werden müssen. Weitere Hinweise zur Proxy-Konfiguration finden sich in der manpage zu `apt.conf(5)`.

11.5.2 univention-updater

Wird `univention-updater` mit dem Parameter ***net*** aufgerufen, wird ein eventuell vorhandenes Repository aktualisiert bzw. ein Release-Update unter Verwendung des konfigurierten Repository-Servers vorgenommen. Neben der Univention Configuration Registry-Variable `proxy/http` wird auch die Umgebungsvariable `proxy_http` berücksichtigt.

11.5.3 univention-security-update

Wird `univention-security-update` mit dem Parameter ***net*** aufgerufen, wird eine Verbindung zum konfigurierten Server für Sicherheitsupdates aufgebaut. Soll für diese Verbindung ein Proxy verwendet werden, kann dies wie bei `univention-updater` über die Univention Configuration Registry-Variable `proxy/http` oder die Umgebungsvariable `proxy_http` erreicht werden. Darüber hinaus kann auch mit der Univention Configuration Registry-Variable `update/security/proxy` die Verwendung eines Proxys konfiguriert werden.

11.5.4 univention-repository-update

Bei der Aktualisierung eines lokalen Repositories mit `univention-repository-update` wird ebenfalls der über `proxy/http` oder die Umgebungsvariable `proxy_http` konfigurierte Proxy-Server verwendet.